Opinnäytetyö (AMK)

Tietojenkäsittelyn koulutusohjelma

Tietoliikenne

2013

Mikko Jokiniemi

TIETOMURROT

- Mitä jokaisen käyttäjän tulisi tietää tietoturvasta ja tietomurroista

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely | Tietoliikenne

Marraskuu 2013 | 75 sivua

Esko Vainikka

Mikko Jokiniemi

TIETOMURROT – MITÄ JOKAISEN KÄYTTÄJÄN TULISI TIETÄÄ TIETOTURVASTA JA TIETOMURROISTA

Tämän opinnäytetyön tarkoituksena on kartoittaa tietomurtojen historiaa, syitä miksi tietomurtoja tapahtuu sekä tietomurroilta suojautumista. Tietoturvassa säästäminen ja käyttäjien tietämyksen puute ovat yleisimmät syyt jotka mahdollistavat tietomurtojen tekemisen, joten työ on laadittu siten, että siitä olisi hyötyä yrityksille sekä yksityishenkilöille.

Opinnäytetyön aihe on hyvin ajankohtainen ja se koskee kaikkia internetiä hyödyntäviä tahoja, yrityksien tietomurtoja tulee jatkuvasti julki eivätkä yksityishenkilötkään ole turvassa tietomurroilta.

Työn empiirinen osuus koostuu tietoturvan osien esittelystä, tietomurtojen menetelmien ja tavoitteiden selvittämisestä sekä siitä, miten käyttäjät voivat välttyä tietomurroilta ja tietovuodoilta.

Opinnäytetyön tuloksena syntyi dokumentaatio, joka on kattava ja helppolukuinen myös peruskäyttäjille. Työn kaksi liitettä käsittelevät tiedostojen suojaamista.

ASIASANAT:

Tietoturva, hakkerointi, tietovuoto, haittaohjelmat

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Technology | Data communications

November 2013 | 75 pages

Esko Vainikka

Mikko Jokiniemi

INFORMATION SECURITY BREACHES – WHAT EVERY USER SHOULD KNOW ABOUT INFORMATION SECURITY AND SECURITY BREACHES

The aim of this thesis is to survey the history of information security breaches, reasons why security breaches occur and how to prevent them. Neglecting information security and lack of knowledge among users are the main factors that make security breaches possible, hence this thesis is made so that it can be utilized by both companies and end users.

Thesis subject is very topical and it affects everyone connected on the internet, company security breaches happen consistently and end users aren't safe from security breaches either.

The empirical part of this thesis consists of introducing the parts that make up the information security, presenting how and why security breaches are happening and how end users can avoid security breaches and data seepages.

As a result of this thesis, a documentation which is informative and easy to comprehend (even to less tech-savvy) was born. As a side product thesis contains two attachment regarding data protection.

KEYWORDS:

Information security, hacking, data seepage, malicious software

SISÄLTÖ

LIITTEET

KUVAT

SANASTO

Anonyymi	Anonyymi-nimitystä käytetään henkilöistä, jotka esiintyvät nimettöminä. Henkilö voi esiintyä anonyymina esim. keskustelufoorumilla tai chatissa, jolloin henkilöä ei pakoteta rekisteröimään käyttäjänimeä, jos kyseinen henkilö ei halua tehdä itseään tunnetuksi. Yleensä anonyymien keskustelijoiden käyttöoikeuksia rajoitetaan. Anonyymille käyttäjälle asetetaan esimerkiksi foorumeiden selaus- ja postitusrajoituksia, joita rekisteröityneillä käyttäjillä ei ole ja henkilöä yritetään täten rohkaista rekisteröimään käyttäjätunnus. Anonymous–termillä voidaan myös viitata saman nimiseen haktivistiryhmään.
Autentikointi	Käyttäjän ja käyttöoikeuksien todentaminen. Todentaminen toteutetaan monesti käyttäjätunnus ja salasana –kirjautumisella.
Backdoor	Takaovi.
Black Hat	Black Hat (Musta Hattu) tarkoittaa hakkeria, joka käyttää hakkerointiosaamistaan tahallisen vahingontekoon. Mediassa esitetyt tietokonerikolliset ovat Black Hat –hakkereita. Tietomurroista puhuttaessa krakkeri ja Black Hat –termit ovat käytännössä verrannollisia toisiinsa, mutta Black Hat –hakkeri nimitystä ei tulisi käyttää krakkerista, joka pelkästään murtaa sovelluksien suojauksia.
Bot	Bot, josta käytetään myös nimitystä botti, on nimitys sovelluksesta, joka osaa toimia itsenäisesti ennalta määritettyjen toimintaohjeiden perusteella. Botit voivat

	suorittaa annetut toiminnot nopeammin kuin ihminen ja ne pystyvät toimimaan taukoamatta. ”Eräs tunnettu esimerkki internetissä käytettävistä boteista ovat hakukoneiden hakurobotit, jotka käyvät itsekseen läpi verkkosivuja, vierailevat niillä ja tutkivat niiltä eteenpäin johtavat linkit, muodostaen näin hakukoneelle tietokannan” (Botti 2013). Toinen esimerkki botista on huijausyrityksen laatima spambot (roskaposti bot), joka osaa omatoimisesti luoda käyttäjätunnuksia foorumeille ja postittaa foorumeille yrityksen mainoksia. Spambot osaa myös lähettää mainospostia sähköpostiosoitteisiin.
Botnet	Bottiverkko.
Bottiverkko	Bottiverkolla tarkoitetaan saastuneista koneista koostuvaa verkkoa. Bottiverkkoa hallitseva(t) henkilö(t) voi yhdellä napinpainalluksella lähettää komennon samanaikaisesti kaikille bottiverkon saastuneille koneille. Bottiverkkojen koneita käytetään usein tahalliseen vahingontekoon mm. roskapostien massapostitukseen ja palvelunestohyökkäyksien suorittamiseen.
Crypting	Kryptaus.
Grey Hat	Grey Hat (Harmaa Hattu)-termillä viitataan hakkereihin, jotka ovat jotain White Hat ja Black Hat –hakkereiden väliltä. Anonymous- ja WikiLeaks–ryhmiä voidaan pitää esimerkkeinä Grey Hat –hakkereista, molemmat tahot ovat tarvittaessa valmiita käyttämään laittomia keinoja saavuttaakseen päämääränsä (esim. valtion salaamien tietojen tuominen julkisuuteen). Grey Hat -hakkereiden toimintatapojen ja tavoitteiden vuoksi heidät voidaan mieltää ”Robin Hood -hakkereiksi”.

Hakkeri

Hakkeri-termi tarkoitti alunperin henkilöä, joka kykeni saavuttamaan päämääränsä tietojärjestelmän rajoituksista huolimatta. Koska nämä kyseiset henkilöt käyttivät ratkaisuja, jotka olivat toisinaan arveluttavia ja nopeasti tehtyjä, ratkaisut saivat nimityksen *hack* (puhekielessä purkkaviritys) ja henkilöt nimityksen *hacker*. (TMRC 2013.)

Hakkeri on yleisnimitys henkilöistä, jotka voivat kiertää tietojärjestelmän rajoituksia, mutta on tärkeää huomioida, että hakkeri –termillä ei aina viitata rikolliseen toimintaan.

Haktivismi

Haktivismi on Internetissä tapahtuvaa aktivismitoimintaa, jolla halutaan saada aikaan huomiota tai muutosta johonkin tiettyyn asiaan. Termi koostuu sanoista hakkeri ja aktivismi. (Hintikka 2013.)

The Anonymous on yksi tunnetuimpia haktivistiryhmiä.

Krakkeri

Krakkeriksi kutsutaan henkilöä, joka murtautuu tietojärjestelmään luvatta. Krakkerilla voidaan myös tarkoittaa henkilöä, joka murtaa tietokonesovellusten suojauksia/tekee luvattomia muutoksia sovellukseen, esim. ”No-CD crack” krakkaukset, joiden avulla voidaan käynnistää sovellus, joka normaalisti vaatisi levyn toimiakseen.

Krakkereista puhuttaessa tarkoitetaan aina Black Hat –hakkereita. Krakkeri omaa saman osaamisen ja tietämyksen kuin hakkeri, mutta krakkeri käyttää osaamistaan tietoisesti vahingontekoon. (The Jargon File 2013a.)

Kryptaus	Kryptaus-termi tarkoittaa salakirjoitusmenetelmää, jolla annetaan lisäsuojaa tiedostolle. Kryptauksen yhteydessä luodaan salausavain, jolla kryptattu tiedosto saadaan myöhemmin avattua. Tavallinen salasana estää ulkopuolista henkilöä avaamasta tiedostoa. Kryptaus puolestaan salakirjoittaa tiedoston sisällön sellaiseen muotoon, etteivät ulkopuoliset henkilöt ymmärrä tiedoston sisältöä. Kryptauksen purkaminen vaatii joko salausavaimen, jonka salauksen tekijä toimittaa vastaanottajille, tai erikseen määriteltyä salasanaa, jonka kryptauksen tehnyt henkilö keksii ja kertoo tiedoston vastaanottajalle.
Saastunut kone	Saastuneella koneella tarkoitetaan konetta, joka on murtautujan hallinnassa tai saastutettu haittaohjelmalla, joka mahdollistaa etähallinnan käyttäjän tietämättä. Saastunutta konetta käytetään usein osana bottiverkkoa.
Takaovi	Takaovi-termillä tarkoitetaan metodia tai mekanismia, jolla ohitetaan tavanomainen autentikaatio ja täten voidaan käyttäjän tietämättä muodostaa etäyhteys kohdekoneelle. Monet haittaohjelmat, etenkin troijalaiset, voivat tehdä koneelle takaovia, joita murtautujat sekä muut haittaohjelmat voivat hyödyntää. (The Jargon File 2013b.) Takaovi–ominaisuus löytyy oletuksena useista etähallinta troijalaisista, mutta muutkin haittaohjelmat voivat käyttää takaovea huomaamattomaan tiedostojen siirtoon ja sovellusten asentamiseen.
Wardriving	Suojaamattomien langattomien verkkojen etsiminen ajoneuvon kanssa sekä löytyneiden verkkojen merkit-

	seminen kartalle. Suosittu aktiviteetti hakkereiden keskuudessa, voidaan mieltää tietomurron pohjatyöksi tai valmisteluksi. (Rouse 2005.)
White Hat	White Hat (Valkoinen Hattu) tarkoittaa hakkeria, joka käyttää hakkerointiosaamistaan tietojärjestelmän haavoittuvuuksien testaamiseen, mutta ei aiheuta vahinkoa järjestelmän sisällä. Yrityksen tietoturva asiantuntija, joka yrittää murtautua yrityksen verkkoon ja dokumentoi tuloksensa on tyypillinen esimerkki White Hat –hakkerista.

1 JOHDANTO

Internet on mahdollistanut nopean ja vaivattoman tiedonsiirron sekä helpottanut tiedonhakua. Sähköposti siirtyy lähettäjältä vastaanottajalle vain muutamassa sekunnissa, kun taas kirjettä tai postikorttia joutuu odottamaan useamman päivän. Yritysten yhteystietoja ei tarvitse enää hakea puhelinluettelosta, sillä Googlen avulla tiedot löytyvät internetistä yhdellä haulla. Pankkiasiat voi hoitaa Internetin ansiosta jonottamatta ja poistumatta kotoa lainkaan. Tiedostoja voi siirtää Dropbox -pilvipalveluun eikä muistitikkua tarvitse kantaa jatkuvasti mukana. Kaikki tämä ja tuhannet muut palvelut ovat mahdollisia internetin ansiosta.

Monista eduistaan huolimatta Internetin käytössä on omat vaaransa: koska internetin käyttö on helppoa, monilta käyttäjiltä helposti unohtuu varovaisuus rahanarvoista ja arkaluonteista tietoa käsitellessä. Salasanojen vaihtamista ja uloskirjautumisen tärkeyttä monesti vähätellään. Entä kuinka moni muistaa joka kerta varmistaa että kirjautui ulos verkkopalvelusta istunnon päätteeksi?

Yksi syy internetin palvelujen varomattomaan käyttöön on käyttäjien tietämyksen puute. Monet käyttäjät eivät ymmärrä, miten arvokkaita heidän palveluidensa tunnukset ja muut tiedot voivat olla ulkopuolisille tahoille. Mitä tapahtuu, jos nämä tiedot päätyvät rikollisille? Kerättyjä tietoja voidaan hyödyntää rikollisiin tarkoituksiin, esimerkiksi laittomiin tilisiirtoihin tai identiteettivarkauksiin. Entä miten rikolliset valitsevat kohteensa ja miten he saavat kohteensa tiedot käsiinsä?

Vaikka yksityishenkilö ei käyttäisikään mitään internetin palveluita, hänen tietokoneensa voi silti osoittautua houkuttelevaksi kohteeksi rikollisille, jos siinä on internet-yhteys. Tietoturvasta huolehtiminen on jokaisen käyttäjän omalla vastuulla eikä sitä tulisi laiminlyödä.

Työn tavoitteena on parantaa lukijan tietämystä tietomurroista, tietomurtojen seurauksista sekä selvittää, miten yleisimmiltä tietomurroilta voidaan välttyä.

2 TIETOTURVAN MÄÄRITELMÄ

Tietoturvan tavoitteena on estää tietomurtoja, rajoittaa tietomurroista syntyvää vahinkoa sekä auttaa tietojärjestelmän toipumista tietomurron jälkeen.

Tietoturvan toteutuminen pohjautuu tietojen luottamuksellisuuteen, eheyteen ja käytettävyyteen. Kyseistä kokonaisuutta nimitetään CIA-kolmikoksi.

Luottamuksellisuus (Confidentiality) tarkoittaa, että tiedot ovat vain asianomaisten henkilöiden käytettävissä. Autentikointi on näkyvin osa luottamuksellisuuden ylläpidosta. (Andress 2011, 4-5.)

Eheys (Integrity) tarkoittaa, että tietoja ei ole luvatta muutettu tai poistettu. Tietojen ja tiedostojen varmuuskopioiden pitäminen ajan tasalla luetaan eheyden ylläpidoksi. (Andress 2011, 5-6.)

Käytettävyys tai saatavuus (Availability) tarkoittaa, että tiedot ovat saatavilla aina, kun niitä tarvitaan. Käyttöoikeudet ja laitteiston ylläpito kuuluvat käytettävyyteen tai saatavuuteen. (Andress 2011, 6.)

CIA:n toteutusta havainnollistetaan vertaamalla CIA:n osia kolmijalkaan: kaikkien osien on oltava tasapainossa, jotta kokonaisuus toimisi. Jos yhtä osaa korostetaan liikaa tai laiminlyödään, tietoturva ei toimi toivotulla tavalla.

Jos luottamuksellisuutta korostetaan liikaa, esimerkiksi antamalla tietojen käyttöoikeudet vain kahdelle henkilölle, käytettävyys tai saatavuus kärsii. Jos kumpikaan oikeutetuista henkilöistä ei ole tavoitettavissa, tietoja ei voida päivittää, mikä puolestaan vaikuttaa tietojen eheyteen. Vastaavasti eheyden liiallinen korostaminen, esimerkiksi tietojen päivittäminen monta kertaa päivässä, tarkoittaa käytännössä liian suurta käyttäjäryhmää. Tämä puolestaan vaarantaa tietojen luottamuksellisuuden. Vastaavasti vapaasti käytettävissä olevat tiedot eivät pysy eheinä pitkään.

3 MERKITTÄVIÄ TIETOMURTOJA

3.1 Ensimmäiset tietomurrot

Ensimmäiset raportoidut tietomurrot tapahtuivat Yhdysvalloissa vuosina 1983 ja 1984. Vuoden 1983 tapauksen kohteena oli New Yorkissa sijaitseva syöpähoitolaitos Memorial Sloan-Kettering. Murtautujat pääsivät tunkeutumaan Digital VAX –tietokoneelle, joka tarkkaili 250 syöpäpotilaan sädehoitoa. Murtautujilla oli vapaa pääsy lääketieteelliseen aineistoon sekä laskutustietoihin. Vuoden 1984 tapaus koskee Los Angelesin TRW-yhtiötä, jonka toimialoihin kuului avaruusteollisuus, autoteollisuus sekä luottotietojen käsittely. Vuoden 1984 murron yhteydessä vietiin arviolta n. 90 miljoonan amerikkalaisen luottotiedot. (Laurio 2009.)

Sloan-Kettering –tapauksen taustalta löytyy 1980-luvun alussa huomiota herättäneen hakkeriryhmän The 414s–ryhmän jäsen Gerald Wondra. Vaikka ryhmän tarkoituksena ei ollut aiheuttaa vahinkoa, murtautuja tuhosi laskutustietoja peitelläkseen omat jälkensä, mistä aiheutui arviolta 1500 dollarin vahingot syöpähoitolaitokselle. (The 414s 2012.)

3.2 Laajimmat tietomurrot

TJX Companies joutui murron kohteeksi vuonna 2005 hakkeri Albert Gonzalezin toimesta, jolloin Gonzalez sekä hänen 11 kumppaniaan aloittivat wardriving ajelunsa ja löysivät TJX Companyn suojaamattoman langattoman verkon. Koska TJX Company ei ollut varautunut siihen, että hakkeri pääsisi heidän järjestelmäänsä sisälle, Gonzalez ryhmineen pystyi kiertämään yhtiön suojatut palvelimet käyttäen sisäänkäyntinä löytämäänsä heikosti suojattua verkkoa. Päästyään paremmin suojatuille palvelimille, hakkeriryhmän oli helppo asentaa palvelimille haittaohjelmia ja tiedonkeruusovelluksia. TJX Companyn palvelimien välistä tiedonsiirtoa ei oltu salakirjoitettu eikä virustorjunnan päivityksistä oltu pidetty huolta. Tietomurto selvisi TJX:lle vasta joulukuussa 2006, lähes kaksi

vuotta murron jälkeen, johon mennessä Gonzalesin ryhmä oli kerännyt arviolta 45,6 miljoonan luottokortin tiedot. (Faustus 2010.)

TJX Company ei kuitenkaan riittänyt Gonzalezille, vuonna 2008 hän kokosi uuden ryhmän ja otti kohteekseen Heartland Payment System -yrityksen. He käyttivät samoja metodeja kuin TJX Companyn tietomurrossa. Gonzalezin ryhmä vei yritykseltä yli 100 miljoonan luotto- ja maksukortin tiedot, minkä ansiosta Heartland Payment Systemin tapaus on tähän mennessä suurin raportoitu tietomurto. Tietomurto paljastui Heartland Payment Systemille vasta, kun Gonzalez pidätettiin toisen rikoksen yhteydessä 7.5.2008. Kuulustelussa Gonzalez tunnusti olleensa yksi TJX Companyyn ja Heartland Payment Systemiin murtautuneista hakkereista. (Faustus 2010.)

Elektroniikkajätti Sony joutui tietomurron kohteeksi vuonna 2011 huhtikuun ja toukokuun aikana. Murtojen arvioidaan tapahtuneen 16-19. huhtikuuta, jona aikana Sonyn tietokannasta varastettiin 77 miljoonan Sony Playstation Network -verkkokaupan käyttäjätilin tiedot. Samoihin aikoihin Sony Online Entertainment (SOE) -verkkopelipalvelu joutui murron kohteeksi, jolloin sieltä vietiin 24 miljoonan käyttäjätunnuksen tiedot. Murtautujat pääsivät Sonyn verkkoon käyttämällä hyväksi Sonyn tietoturvassa havaittua haavoittuvuutta, josta Sony tiesi jo ennen murtoja ja jota ei oltu korjattu. (Edwards & Riley 2011.)

Tammikuussa 2013 Sony Computer Entertainment Europe sai Iso-Britannian Information Commissioner's Office –organisaatiolta 400,000 dollarin rikesakon asiakkaiden yksityisyydensuojan vaarantamisesta sekä tietoturvan laiminlyönnistä (McMillan 2013).

4 TIETOMURTOJEN MOTIIVIT

Ensimmäisistä raportoiduista tietomurroista voidaan päätellä muutama syy tietomurtojen tapahtumiselle: Sloan-Kettering -tapauksessa kyseessä oli harmiton pila, joka ryöstäytyi käsistä. Hakkeriryhmä harrasti hakkerointia sen tuoman jännityksen sekä näyttämisen halun vuoksi. Näyttämisen halu on yleistä myös virustehtailijoiden keskuudessa. Tarkoituksena ei välttämättä ole aiheuttaa rahallista vahinkoa vaan todistaa muille pystyvänsä murtautumaan haluamaansa kohteeseen. Murtojen yhteydessä voi kuitenkin syntyä tahatonta vahinkoa ja pelkkä murron yritys on rangaistava teko. Esimerkiksi pelkkä salasanojen arvailu lasketaan murtoyritykseksi.

TRW-yhtiön tapauksessa hakkerin, tai hakkereiden, motiivina oli tahallinen vahingonteko. Tietovuodon välittömänä seurauksena oli yrityksen maineen ja asiakkaiden menetys, mikä puolestaan lisää kilpailevien yritysten markkinaosuutta. On tärkeää huomioida, että TRW-yhtiön toimialoihin kuului myös avaruusteollisuus. Kyseinen yhtiö rakensi muun muassa tiedustelusatelliitteja Yhdysvaltojen asevoimille, joten on hyvin mahdollista, että tietomurron syynä olisi voinut olla teollisuusvakoilu.

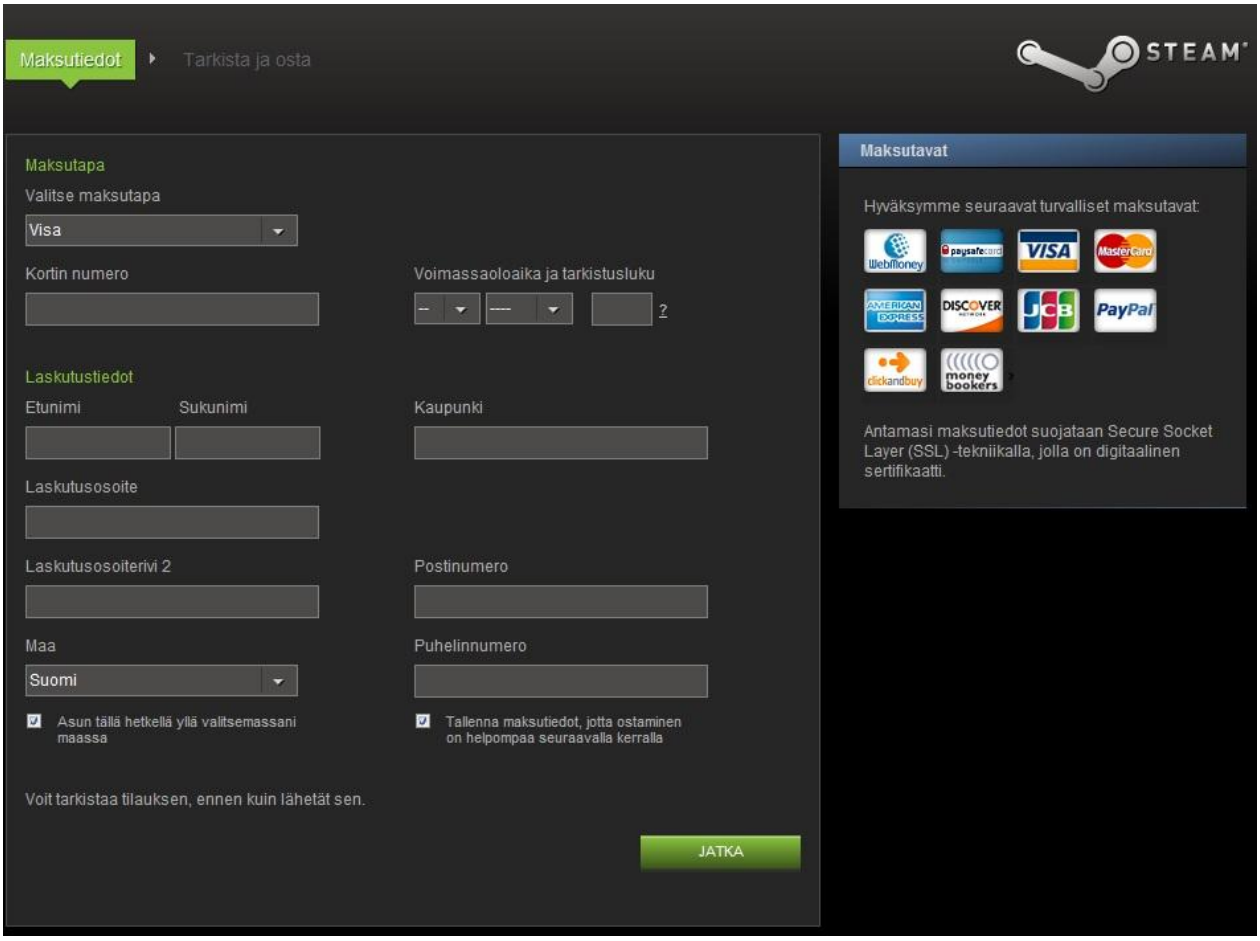
Kaikkien tietomurtojen motiivina ei välttämättä ole taloudellinen hyöty eikä harmiton pilailu. Julkisuuden henkilöitä ja maailman tapahtumia koskevia tietoja etsitään joka päivä uutisotsikoista, mutta journalistit eivät aina kerro koko totuutta: WikiLeaks on tuonut julkisuuteen useita dokumentteja ja videoita, joita valtiot ovat yrittäneet pitää salassa. Yksi tunnetuimpia vuotoja on videomateriaali, joka on kuvattu 7. heinäkuuta 2007 Bagdadin ilmaiskuista, joissa Yhdysvaltojen helikopterit ampuivat 12 irakilaista siviiliä luultuaan heidän olevan aseistautuneita. WikiLeaks on saanut sekä kritiikkiä että positiivista palautetta toiminnastaan. Viranomaiset ovat kritisoineet WikiLeaksia kansallisen turvallisuuden vaarantamisesta, kun taas monet Yhdysvaltojen lehdet, mm. New York Daily News ja TIME, ovat ylistäneet WikiLeaksin toimintaa.

5 KOHTEIDEN VALIKOITUMINEN

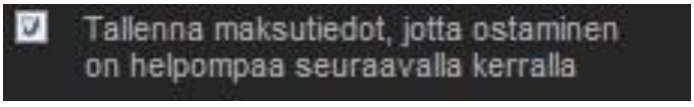
Taloudellinen hyöty on näkyvin tekijä murtokohdetta valittaessa. Pankit ja luottoyritykset ovat tämän vuoksi houkuttelevia kohteita, koska murtautuja saa taloudellisen hyödyn suoraan itselleen sen sijaan, että hän tekisi tietomurron toimeksiantona. Pankit ja luottoyhtiöt tietävät turvallisuudella olevan niinkin suuren merkityksen, että asiakas saattaa mennä toisen pankin tai luottoyhtiön asiakkaaksi, jos asiakkaan mielestä säästöt eivät ole turvassa heidän pankissaan tai jos luottokorttia ei ole turvallista käyttää. Tästä syystä pankit ja luottoyhtiöt yleensä huolehtivat tietoturvastaan varsin kiitettävästi.

Verkkokaupat ovat suosittuja kohteita samanlaisista syistä. Kortilla maksettaessa riittää, kun tilauksen yhteydessä ilmoittaa verkkokaupalle maksukortin numeron, kolminumeroisen tarkistusluvun joka löytyy kortin kääntöpuolelta kortin voimassaoloajan (Kuva 1). Verkkokaupasta tilattaessa ei tarvitse syöttää kortin PIN-koodia eikä tilausta tarvitse vahvistaa erikseen turvaluvulla kuten verkkopankissa. Maksu veloitetaan suoraan asiakkaan tililtä. Toisin sanoen, jos asiakkaan kortti tai kortin tiedot ja käyttäjätunnus päätyvät rikollisen käsiin, mikään ei estä rikollista ostamasta tavaroita asiakkaan laskuun, jos asiakas ei ole huomannut kortin katoamista ja kuolettanut korttiaan ajoissa. Maksutietojen väärinkäytön välttämiseksi käyttäjän tulisi välttää verkkokauppojen maksutietojen tallentamistoimintoa (Kuva 2).

Koska maksutapahtumat tallentuvat verkkokaupan palvelimille, rikollinen voi valita murtautuuko hän palvelimelle ja varastaa useita käyttäjätunnuksia ja maksutapahtumien tositteita vai murtautuuko hän käyttäjän koneelle ja selvittää yksittäisen käyttäjän maksutiedot. Tämä puolestaan tekee yksittäisten henkilöiden koneista houkuttelevia kohteita. Saatava taloudellinen hyöty saattaa jäädä pienemmäksi, mutta yksittäisten käyttäjien koneiden tietoturva on yleensä huomattavasti heikommalla tasolla kuin yrityksissä.



Kuva 1. Näkymä Steam-verkkokaupan maksutavoista.



Kuva 2. Helppokäyttöisyystoiminto, josta saattaa koitua vahinkoa käyttäjälle.

Hakkerointia voidaan hyödyntää myös yritys- ja teollisuusvakoilussa, joka tekee käytännössä mistä tahansa yrityksestä tai yrityksen työntekijän koneesta houkuttelevan kohteen. Tämän vuoksi on erityisen tärkeää, että yritykset laativat tietokoneen käyttöä koskevia sääntöjä ja käytäntöjä, joilla vältyttäisiin mahdollisilta tietomurroilta ja tietovuodoilta. Yhden työntekijän tahaton virhe voi olla yhtä suuri uhkatekijä yrityksen tietoturvalle kuin osaava hakkeri.

Tästä esimerkkinä vuonna 2008 Ruotsissa kohua aiheuttanut tapaus, jossa kirjastoon unohtuneelta muistitikulta löytyi salaiseksi luokiteltuja sotilastietoja. Do-

kumenttien joukosta löytyy muun muassa analyysi Afganistanissa tapahtuneesta hyökkäyksestä, jonka seurauksena kaksi ruotsalaista eliittisotilasta menetti henkensä. Dokumenttien joukosta löytyi myös tiedusteluraportti amerikkalaisesta turvayhtiöstä. (Cantwell 2008.)

Teollisuusvakoilun ohella tahallinen vahingonteko on valitettavan yleinen ilmiö. Yrityksen tiedostojen ja tietokantojen varastaminen tai tuhoaminen ei ole enää uusi ilmiö. Sitä vastoin teollisuusjärjestelmiä sabotoivat haittaohjelmat ovat vielä tuore ilmiö, johon ei ole osattu varautua.

Stuxnet on oiva esimerkki tämän tyyppisistä haittaohjelmista. Stuxnet aiheutti suurta vahinkoa Iranin ydinvoimaloissa sammuttaen automaattisesti Siemensin valmistamia laitteita. Stuxnet oli räätälöity leviämään ydinvoimaloiden kaltaisiin ympäristöihin, jotka eivät ole kiinni Internetissä. Mato osasi levitä usb-muistien välityksellä ja hyödynsi leviämisessään myös Windowsin ennestään tuntematonta tulostimien verkkojaon haavoittuvuutta. (Krebs 2010.)

Voimme olettaa, että tämänkaltaisia haittaohjelmia tullaan näkemään jatkossakin. Stuxnet osoitti, että tietoturvasta tulisi huolehtia myös sellaisissa verkkoympäristöissä, jotka eivät ole kytköksissä Internetiin.

6 HAITTAOHJELMIEN VAIKUTUS TIETOTURVAAN

Haittaohjelmilla voidaan edesauttaa tietomurron toteuttamista ja joissakin tapauksissa haittaohjelmaa voidaan käyttää tietomurron sijaan aiheuttamaan vahinkoa. Virukset kykenevät tuhoamaan sovelluksia ja tiedostoja niinkin tehokkaasti, että tietokoneesta tulee käyttökelvoton. Esimerkiksi CIH-virus joka ylikirjoittaa koneen BIOS-muistin. Jos BIOS-muisti on lukukelvoton, niin tietokone ei pysty enää käynnistämään itseään. Urkintaohjelmilla voidaan selvittää käyttäjien salasanoja. Koska haittaohjelmia on tehtailtu moneen eri käyttötarkoitukseen, on tärkeää ymmärtää, miten ne eroavat toisistaan. Haittaohjelmien vaikutuksia verrataan tietoturvan CIA-kolmion osioihin sekä selitetään, miksi kyseiset haittaohjelmat vaikuttavat juuri näihin tietoturvan osioihin.

6.1 Virus

Virus on haittaohjelmatyypeistä tunnetuin. Virukseksi luokitellaan haittaohjelma, joka osaa levittää kopioita itsestään muihin koneisiin ja osaa tuhota koneen tiedostoja. Koska virus vaatii käynnistyskomennon käyttäjältä, virukset naamioidaan yleensä hyötyohjelmiksi, peleiksi tai sähköpostien liitetiedostoiksi, mitä on helppo säilyttää ja siirtää paikasta toiseen muistitikulla tai sähköpostilla. Naamioidulla tiedostolla on helppo huijata käyttäjä käynnistämään saastutettu tiedosto. (Symantec 2012.)

Viruksia on monenlaisia. Osa viruksista on harmittomia pilailuviruksia, esimerkiksi DOS-käyttöjärjestelmän Ambulance-virus, kun taas toiset virukset pyrkivät tuhoamaan tai ylikirjoittamaan koneen järjestelmätiedostoja, kuten edellä mainittu CIH-virus. Viruksien haittavaikutuksilta voidaan välttyä pitämällä virustorjuntasovelluksen tunnistetiedot ajan tasalla. Jos käyttäjä on epävarma tiedoston turvallisuudesta, hänen kannattaa kiinnittää huomiota seuraaviin asioihin:

- Tiedoston pääte. Esimerkiksi, jos tiedoston nimi on ”dokumentti.doc.exe” tiedostoa ei kannata avata.
- Tiedoston koko ja muokkauspäivämäärä. Vertaa tiedoston nimeä käyttöjärjestelmän omiin tiedostoihin, esimerkiksi Sys32- kansion tiedostot.
- Tiedoston nimi. Kirjoita tiedoston tai sovelluksen nimi Googleen ja selvitä hakutuloksista onko tiedosto tai sovellus turvallinen.
- Internetistä ladattu tiedosto. Selvitä, miltä sivulta tiedosto on ladattu.

Vaikutus CIA-kolmioon: Yleensä virukset vaarantavat tietojen saatavuuden ja tietojen eheyden. Eheys menetetään, jos virus ylikirjoittaa tai muuttaa tiedoston sisällön. Saatavuus puolestaan menetetään, jos virus poistaa tiedostoja. Virukset eivät suoranaisesti vaikuta autentikointiin, joten luottamuksellisuus ei kärsi viruksista, kuten saatavuus ja eheys.

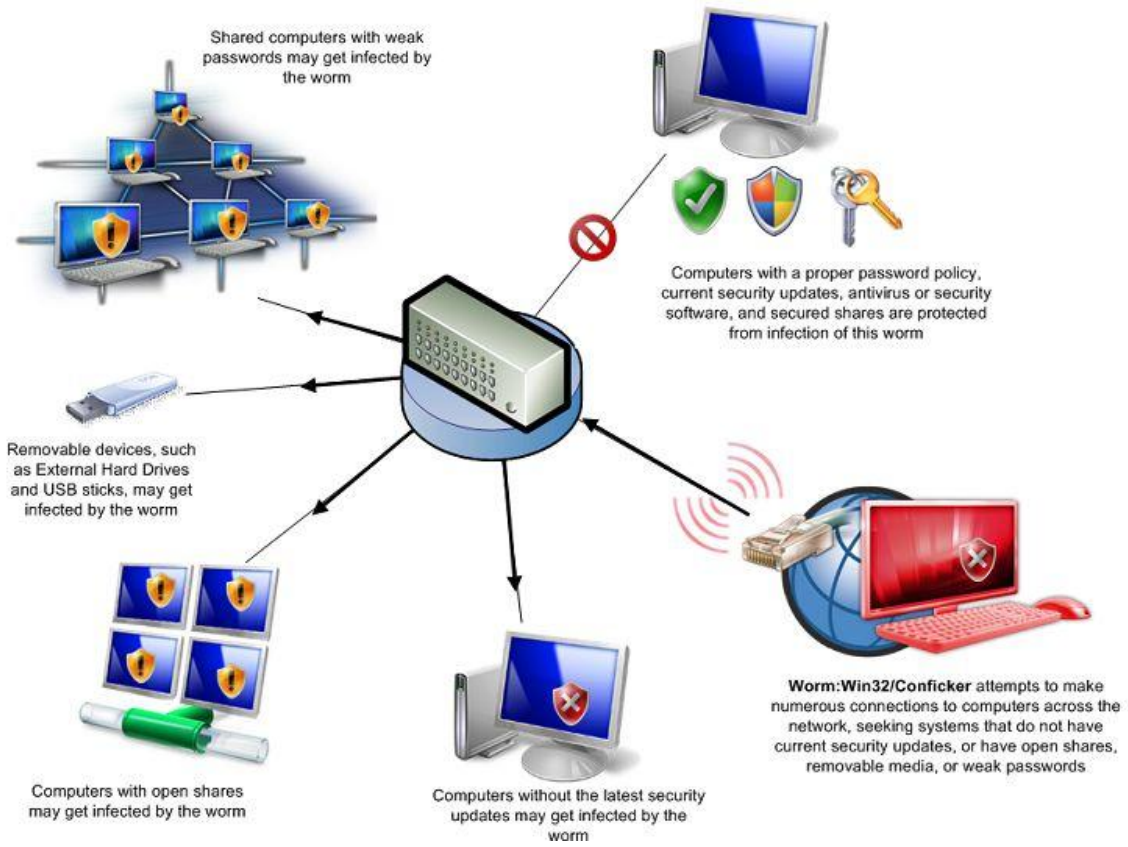
6.2 Mato

Mato eroaa viruksesta levittäytymiskeinonsa ja toimintansa vuoksi: Mato vaatii toimiakseen yhden saastuneen koneen, johon mato alkaa replikoimaan itseään täyttäen koneen kiintolevyn. Tämän jälkeen mato alkaa levittäytyä verkon muihin koneisiin ja jaettuihin verkkoresursseihin, esimerkiksi verkkolevyihin. Mato leviää saastuneelta koneelta muihin koneisiin käyttäen joko käyttöjärjestelmän haavoittuvuuksia tai sähköpostin osoitelistaa, minkä jälkeen nämä muut saastuneet koneet toistavat samat toimenpiteet. (Symantec 2012.)

Ensimmäinen mato, Morris Worm, sai alkunsa marraskuun 2. päivä 1988, kun Cornellin yliopiston opiskelija, Robert Tappan Morris, yritti kehittää ohjelman, jolla voitaisiin mitata Internetin koko. Ohjelma hyödynsi tunnettuja haavoittuvuuksia sekä osasi ohittaa heikolla salasanalla suojattuja autentikointeja. Ohjelma oli kuitenkin suunniteltu siten, ettei sen olisi pitänyt pystyä vaikuttamaan oikeaoppisesti suojattuun tietojärjestelmään.

Ohjelmakoodissa oli kuitenkin ohjelmointivirhe, jonka vuoksi ohjelma ei toiminut siten kuin sen olisi pitänyt. Tämä teki ohjelmasta vaarallisemman kuin Morris oli kuvitellut: se pystyi monistamaan itsensä samalle koneelle useaan kertaan ja kone hidastui sitä mukaa, kun mato kopioi itse itsensä saman koneen sisällä, tehden koneesta käyttökelvottoman koneen resurssien loputtua. Madon arvioidaan tehneen tuhoja kaiken kaikkiaan 100,000–10,000,000 dollarin edestä. Morris tuomittiin kolmeksi vuodeksi ehdonalaiseen, 400 tunniksi yhdyskuntapalveluun sekä 10,000 dollarin sakkoon. (FindingDulcinea 2013.)

Levittäytymiskykynsä ansiosta mato voi ruuhkauttaa web-palvelimia ja työasemia niin pahasti, että ne lakkaavat toimimasta ja vaativat uudelleenkäynnistyksen toimiakseen, toisin sanoen madolla voidaan toteuttaa palvelunestohyökkäys ilman bottiverkkoa kohdeverkon sisäpuolelta.



Kuva 3. Win32 Conficker -madon toimintaperiaate (Microsoft 2013).

Haittaohjelmien tekijät saattavat käyttää matojen levittäytymiskykyä (Kuva 3) hyödykseen muiden haittaohjelmien levittämiseen, mikä moninkertaistaa madon aiheuttaman tietoturvauhan. Paras keino suojautua madoilta on pitää koneen tai koneiden palomuuri ja virustorjuntasovellus ajan tasalla. Lisäksi kannattaa olla tarkkana sähköpostin liitetiedostojen kanssa, sekä ilmoittaa työkaverille etukäteen, jos aikoo lähettää hänelle sähköpostin, jonka mukana on liitetiedosto. Monesti tämän käytännön toteutumista on vaikea seurata työpaikoilla, etenkin jos kyseessä on iso firma, jonka vuoksi tämä käytäntö toteutuu vain harvoilla työpaikoilla.

Vaikutus CIA-kolmioon: Madon päätarkoituksena on ruuhkauttaa verkkoliikennettä ja tukkia verkossa olevien koneiden kiintolevyt. Jos verkko on ruuhkautunut, niin koneiden ja laitteiden välinen kommunikaatio hidastuu tai lakkaa toimimasta, joka puolestaan haittaa tietojen saatavuutta. Tämä koskee kaikkea verkossa tapahtuvaa liikennettä. Pahimmillaan verkon ruuhkautuneisuus saattaa estää käyttäjää kirjautumasta verkkoon, jos koneen ja kirjautumispalvelimen välinen yhteys on ruuhkautunut. Tässä tapauksessa käyttäjien autentikointi ei toimi. Vaaralliset madot voivat varastaa kirjautumistietoja tai ylikirjoittaa koneen tiedostoja. Jos mato varastaa kirjautumistietoja, rikollinen pääsee kirjautumaan tietokoneelle tai verkkoon ongelmitta ja hänellä on vapaa pääsy käyttäjätunnuksen käyttöoikeuksien sallimiin tietoihin, esimerkiksi tietojen varastamiseen, muokkaamiseen tai poistamiseen.

6.3 Troijalainen

Troijalainen on haittaohjelma tai ohjelmapätkä, joka on naamioitu hyötyohjelmaksi. Troijalainen aktivoituu vasta sen jälkeen, kun käyttäjä on asentanut niin sanotun hyötyohjelman koneelle, toisin sanoen käyttäjä huijataan asentamaan troijalaista kantava sovellus koneelle.

Troijalaisen aiheuttamat tuhot vaihtelevat suuresti. Osa troijalaisista aiheuttaa käyttäjälle kiusaa vaihtamalla työpöydän taustakuvaa, kun taas toiset troijalaiset avaavat koneen portteja ja takaovia, joiden avulla murtautujat voivat ohittaa ko-

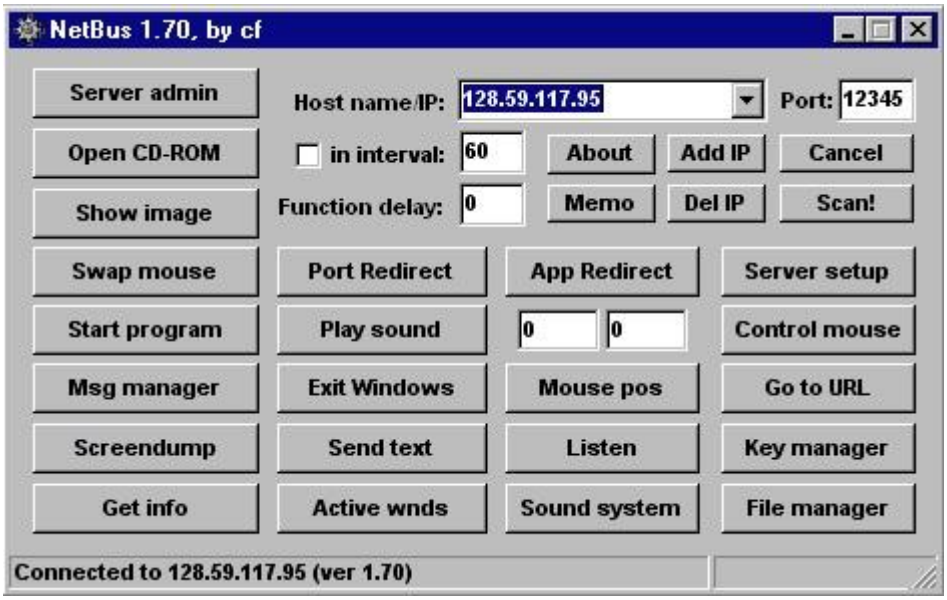
neen palomuurin sekä virustorjunnan ja pääsevät tämän ansiosta käyttäjän huomaamatta koneen tiedostoihin käsiksi. Troijalaiset voivat myös viruksen tavoin tuhota tai muokata tiedostoja, mutta viruksista ja madoista poiketen troijalaiset eivät pysty levittämään itseään koneelta toiselle. Poikkeuksena tietenkin tilanne, jossa sama käyttäjä tietämättään asentaa saman troijalaisen usealle koneelle. (Symantec 2012.)

Etähallinta –troijalainen

Etähallinta–troijalaista, joista käytetään myös nimitystä Backdoor–troijalainen, voidaan hyödyntää tietomurron tekemisessä. Jos koneelle on asennettu etähallinta–troijalainen, murtautuja voi tehdä kohdekoneella seuraavia toimenpiteitä (Kuva 4 ja Kuva 5):

- Tiedostojen hallinta, sis. tiedostojen lataaminen koneelta tai koneelle, tiedostojen tuhoaminen sekä sovellusten käynnistäminen.
- Koneen rekisteritietojen muokkaus.
- Kuvakaappaus ja web-kameran kaappaus.
- Koneelle tallennettujen salasanojen haku.
- Koneen sammutus, uudelleenkäynnistys, uloskirjaus ja muut virranhallintaominaisuudet. (Rajnish 2012.)

Kuva 4. Beast -troijalaisen hallintasovellus (Beast Trojan horse 2012).



Kuva 5. NetBus -troijalaisen hallintasovellus (Ethicalhack3r 2013).

Etähallinta–troijalaiset voivat olla erittäin vaarallisia, jos niiden olemassaoloa ei huomata riittävän ajoissa. Etähallinta–troijalainen voi toimia pitkään passiivisena tarkkailutyökaluna, joten käyttäjän on usein lähes mahdotonta havaita, onko koneella haittaohjelmaa, jos kone muutoin toimii normaalisti. Vaikka käyttäjä

alkaisi jälkeenpäin epäillä haittaohjelman olemassaoloa, virustorjunta- tai palomuurisovelluksen lataaminen ja asentaminen koneelle on tässä vaiheessa jo liian myöhäistä, koska murtautuja voi halutessaan estää käyttäjää tekemästä koneellaan yhtään mitään, esimerkiksi sammuttamalla koneen tai estämällä sovelluksia käynnistymästä. Käyttäjä voi katkaista etähallinnan kytkemällä koneen pois internetistä, mutta tämä ei poista troijalaista koneelta.

Etähallinta–troijalaisesta pääsee eroon pienimmällä vaivalla asentamalla virustorjuntasovelluksen sekä tuoreet virustunnisteet ulkoisesta massamuistista, kuten muistitikulta tai ulkoiselta kiintolevyltä, kun kone ei ole kytkettynä internetiin, ja suorittamalla skannauksen koneen ollessa vikasietotilassa. Jos tämä ei ole mahdollista, vaihtoehdoiksi jäävät joko haittaohjelman tai saastuneiden tiedostojen poistaminen käsin vikasietotilassa tai koneen käyttöjärjestelmän uudelleenasennus ja aiemman levyosion tuhoaminen.

Pankkitroijalainen

Etähallinta–troijalaisen lisäksi pankkitroijalaiseksi nimitetty Zeus –troijalainen sekä Zeuksen variaatiot ovat tähänastisista troijalaisista kenties vaarallisimpia. Zeuksen tunnistamisesta teki erityisen vaikeaa se, että Zeus käytti Kaspersky–tietoturvayhtiön tuottaman sovelluksen väärennettyä sertifikaattia. Sovellusvalmistajat lisäävät sovelluksiinsa sertifikaatin, joka varmistetaan asennuksen yhteydessä. Sertifikaatti toimii virallisena leimana, josta tunnistaa kyseessä olevan sovellusvalmistajan hyväksymä tuote. Sertifikaatin takia virustorjuntaohjelmat eivät tunnistaneet koneelle asennettua Zeus–troijalaista. (Kirk 2010.)

Zeus–troijalaisen ominaisuuksiin kuuluu näppäimistön painallusten tallentaminen, web–selaimen kaavatietojen kaappaaminen sekä kerättyjen tietojen lähettäminen eteenpäin ennalta määrättyyn kohteeseen. Näiden ominaisuuksien ansiosta Zeusta voidaan käyttää erinäisten palveluiden tunnuksien varastamiseen, myös sellaisten palveluiden, joiden tietoturvaa on vaikea murtaa. Tästä syystä pankkitroijalainen-nimitys. Pankin järjestelmiin murtautumisen sijaan rikollinen

voi varastaa tarvitsemansa tiedot suoraan käyttäjän saastuneelta koneelta ja siirtää rahaa uhrin tililtä jäämättä kiinni.

Koska troijalaisista, etenkin etähallinta–troijalaisista, voi olla hankalaa ja työlästä päästä eroon, paras keino välttyä vahingoilta on estää troijalaisten pääsy koneelle sekä estää niiden käynnistyminen. Virustorjuntaohjelmat ilmoittavat käyttäjälle havaitsemistaan haittaohjelmista, tämän vuoksi tunnistetiedostot kannattaa pitää ajan tasalla.

Jos koneen toiminnassa esiintyy jotain, joka viittaa troijalaiseen, kone on syytä kytkeä irti internetistä ja käynnistää virustorjuntaohjelman skannaustoiminto välittömästi. Troijalaiseen viittaavia toimintoja ovat muun muassa työpöydän taustakuvan vaihtuminen itsestään, koneen hidastelu ilman näkyvää syytä tai koneen levykelkan aukeaminen omia aikojaan. Koneen uudelleenkäynnistäminen vikasietotilaan parantaa haittaohjelman löytymisen todennäköisyyttä.

Jos virustorjuntaohjelma ei poista troijalaista kokonaan, Internetistä löytyy lisäohjeita troijalaisen poistamiseen. Monet tietoturvayhtiöt valmistavat räätälöityjä haittaohjelmien poistotyökaluja poikkeuksellisen hankalia troijalaisia vastaan.

Vaikutus CIA-kolmioon: Troijalaiset mahdollistavat käyttäjän salasanojen keräämisen sekä koneen etähallinnan. Näiden toimintojen ansiosta voidaan ohittaa käyttäjän tunnistaminen, joka puolestaan johtaa luottamuksellisuuden menetykseen. Tiedostojen poistamisen ja muokkaamisen lisäksi troijalaiset mahdollistavat myös tiedostojen kopioimisen, mikä tarkoittaa tietojen eheyden sekä saatavuuden vaarantumista. Koska troijalainen pyrkii olemaan käyttäjälle näkymätön haittaohjelma, troijalaisia harvoin käytetään helposti havaittavien toimintojen, kuten tiedostojen poistaminen, suorittamiseen.

6.4 Adware

Adwarella tarkoitetaan mainosohjelmaa, joka esittää käyttäjälle mainoksia tietyn sovelluksen suorittamisen aikana. Adware–sovellus voi asentua koneelle net-

tiselaamisen yhteydessä ja mainosohjelmia voi tulla myös ilmaisohjelmien mukana. (Symantec 2012.)

Adware itsessään ei ole kovin vaarallinen, mutta adwareen voidaan integroida muita haittaohjelmia, esimerkiksi spywarea, tai mainos voi johdattaa käyttäjän sivuille, joista tarttuu haittaohjelmia koneelle. Tämän vuoksi näennäisesti vaaraton mainosohjelma voikin osoittautua tietoturvan uhkatekijäksi. Tästä syystä adwaren poistaminen ei ole huono idea vaikka se ei näyttäisikään haittaavan koneen käyttöä.

Vaikutus CIA-kolmioon: Adware ei itsessään vaaranna tietoturvaa, mutta adwareen integroidut haittaohjelmat aiheuttavat vahinkoa. Adwaren vahingot riippuvat pitkälti siitä, mitä haittaohjelmia adwareen on integroitu.

6.5 Spyware

Spywarella tarkoitetaan haittaohjelmaa, joka kerää tietoja käyttäjästä, itse tietokoneesta tai käyttäjän Internet–selaimen käytöstä ja lähettää kerätyt tiedot kolmannelle osapuolelle. Spyware voi myös ladata ja asentaa muita haittaohjelmia koneelle käyttäjän tietämättä, mikä puolestaan varaa koneen levytilaa ja käyttömuistia. Vähäinen levytilan ja käyttömuisti ilmenevät käyttäjälle koneen hidasteluna. Yleisin syy, miksi spyware -haittaohjelmia päätyy käyttäjän koneelle, ovat internetin ilmaisohjelmat. Jos ohjelman lataa epäluotettavalta sivulta, on mahdollista, että sovelluksen lisäksi koneelle asentuu käyttäjän tietämättä haittaohjelmia. (Symantec 2012.)

Tämän vuoksi on tärkeää kiinnittää huomiota, miltä sivuilta lataa tiedostoja ja skannata ladatut tiedostot ennen sovelluksen asentamista.

Vaikutus CIA-kolmioon: Spywaren päätarkoitus on kerätä käyttäjästä tietoja ja lähettää tiedot eteenpäin. Kerätyt tiedot saattavat olla arkaluonteisia, jonka vuoksi tietojen välittäminen eteenpäin saattaa vaarantaa tietojen luottamuksellisuuden. Spyware aiheuttaa toiminnallaan monesti koneen hidastelua. Koneen hidastelu haittaa tietojen saatavuutta yksittäisen käyttäjän osalta, mutta spywa-

ren vaikutus verkon toimintaan on huomattavasti vähäisempi kuin madoilla. Spyware ei itsessään muokkaa, poista tai ylikirjoita koneen tiedostoja. Toisaalta, jos spyware asentaa koneelle muita haittaohjelmia, niin spyware saattaa epäsuorasti vaarantaa tietojen eheyden.

6.6 Roskaposti

Roskaposti mielletään yleensä pelkäksi ärsykkeeksi, mutta suurina määrinä roskaposti voi tukkia postilaatikon ja estää asiallisen sähköpostin vastaanottamisen (Symantec 2012).

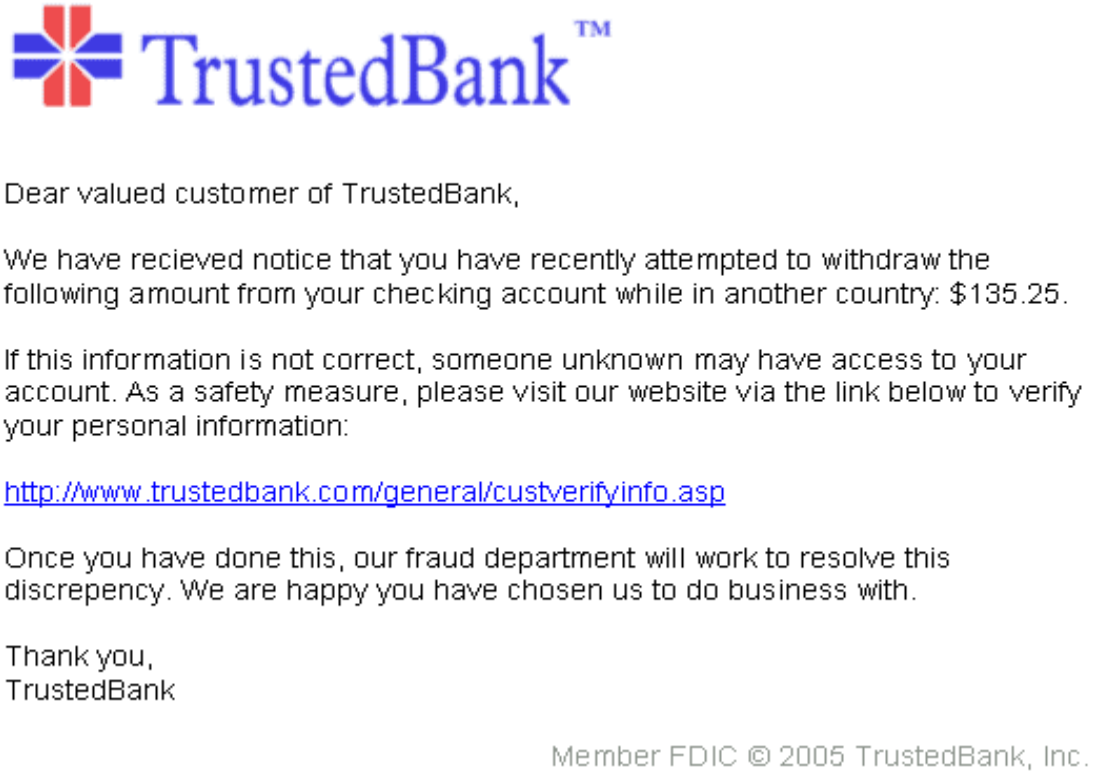
Roskapostia käytetään yleensä joko virusten tai matojen välittämiseen, huijausyritysten mainontaan tai phishing–tietojenkalasteluun, joten roskapostin vaarallisuutta ei tulisi vähätellä. Koska roskapostin lähettäminen on ilmaista ja lähettämisen voi helposti automatisoida boteille, yksikin roskapostittaja voi helposti lähettää satoja, tai jopa tuhansia, roskaposteja päivässä.

Roskapostia esiintyy niin yksittäisten käyttäjien kuin yritysten työntekijöiden koneilla. Yksittäisten käyttäjien joukosta löytyy aina joku, joka erehtyy luulemaan roskaposteja asiallisiksi viesteiksi. Työpaikoilla sähköpostilaatikon tukkiminen voi estää työasioiden hoitamista. Roskapostista pääsee helpoiten eroon poistamalla ne saman tien. Jos käyttäjä kuitenkin avaa viestin, niin viestin linkkejä ja mahdollisia liitetiedostoja ei missään nimessä tulisi avata. Huonolla onnella käyttäjä vahingossa lataa viruksen tai madon koneelleen tai käyttäjä päätyy roskapostittajien massapostituslistalle parilla huolimattomalla hiirenpainalluksella.

Monissa yrityksissä ja Internetin sähköpostipalveluissa on käytössä omat roskapostisuodattimet, mutta suodattimista huolimatta käyttäjälle voi tulla päivittäin muutama roskaposti. Käyttäjä voi halutessaan lisätä sähköpostiin omat suodattimet, joilla roskapostin tulon saa yleensä loppumaan.

Etenkin phishing-tietojenkalasteluviestit olisi hyvä tunnistaa mahdollisimman ajoissa ja poistaa ne saman tien sähköpostista. Phishing-viestin lähettäjä pyrkii

esiintymään yrityksen työntekijänä, yleensä järjestelmänvalvojana, ja kysyy viestin vastaanottajalta hänen henkilötietojaan tai käyttäjätunnuksen salasanaa. Vaihtoehtoisesti viestin lähettäjä kirjoittaa viestiinsä ”käyttäjätunnuksesi on vaarassa, käy vaihtamassa salasanasi välittömästi välttyäksesi vahingoilta” ja lisää viestiin linkin, joka johtaa käyttäjän sisäänkirjautumissivulle. Nämä sisäänkirjautumissivut näyttävät lähes identtisiltä palvelujen virallisten sivujen kirjautumisnäkymän kanssa, mutta tosiasiassa väärennetyt sisäänkirjautumissivut lähettävät käyttäjän tiedot suoraan kalastelijalle (Kuva 6).



Kuva 6. Esimerkki phishing –viestistä (McDonough 2013).

Phishing–kalastelu käyttää hyväkseen käyttäjän tietämättömyyttä. Yritykset eivät koskaan kysele asiakkailtaan heidän käyttäjätunnuksiensa tietoja, koska yrityksen työntekijät voivat selvittää tarvitsemansa tiedot omista järjestelmistään.

Phishing-viestejä voidaan myös lähettää tunnettujen yritysten nimissä, koska sähköpostin lähettäjä ja viestipohja on helppo väärentää. Paras keino välttyä vahingoilta on olla avaamatta mitään viestin linkkejä ennen kuin on varmistanut

kyseessä olevan virallisen yrityksen lähettämä viesti, joko hakukoneen tai keskustelufoorumien avulla.

Jos kyseessä on tunnettu yritys, mutta viestin turvallisuudesta ei voi olla varma, käyttäjä voi aina lähettää sähköpostia yrityksen asiakaspalveluun ja kysyä onko kyseessä heidän lähettämä viesti vai phishing-viesti.

Vaikutus CIA-kolmioon: Suurina määrinä roskaposti ruuhkauttaa sähköpostipalvelimen, mikä estää sähköpostien lähettämisen ja vastaanottamisen sekä tekee käyttäjien sähköpostilaatikoista hankalasti käytettäviä. Molemmat haittatekijät vaikuttavat tietojen saatavuuteen. Phishing-viesteillä kalastetut käyttäjätunnukset ja salasanat puolestaan vaarantavat tietojen luottamuksellisuuden, kun taas roskapostin liitetiedostoista voi tarttua haittaohjelmia, jotka vaarantavat tietojen eheyden.

6.7 Scareware eli Rogueware

Scareware, josta käytetään myös nimitystä Rogueware, on nimensä mukaisesti haittaohjelmatyyppi, joka käyttää hyväkseen pelottelua. Scareware–sovelluksen mainos tulee käyttäjän näytölle, joko tietylle nettisivulle mentäessä tai koneelle asentuneen adwaren ansiosta antaen käyttäjälle valheellisen ”Koneesi on vaarassa! Korjaa koneesi asentamalla tämä ohjelma!” -ilmoituksen ja ohjaa käyttäjän kyseisen sovelluksen kotisivuille (Kuva 7).

Jos käyttäjä luulee ilmoituksen pitävän paikkansa, hän lataa sovelluksen ja asentaa sen koneelleen saman tien perehtymättä ohjelman toimintaan sen tarkemmin. Nämä huijausohjelmat pyrkivät imitoimaan ulkoasunsa puolesta oikeita virustorjuntasovelluksia. Tästä syystä peruskäyttäjän voi olla hyvin vaikeaa erottaa huijausohjelmaa oikeasta virustorjuntasovelluksesta. Asentamisen jälkeen huijausohjelma skannaa koneen ja esittää löytäneensä lukuisia haittaohjelmia, sekä kehottaa käyttäjää ostamaan ohjelman täysversion, jolla voi poistaa havaitut haittaohjelmat. Scarewaren asentamisen yhteydessä koneelle voi asentua muita haittaohjelmia, esim. troijalainen.

Scarewaren tehokkuus perustuu käyttäjän pelon hyväksikäyttöön. Jos koneen näytölle ilmestyy kesken kaiken ilmoitus koneella piilevästä haittaohjelmasta, moni käyttäjä hätääntyy ja asentaa huijausohjelman saman tien. Käyttäjä huijataan luulemaan, että haittaohjelmasta pääsee heti eroon, kun asentaa näytöllä mainostetun virustorjuntasovelluksen, vaikka tosiasiassa sovelluksen asentamisesta on käyttäjälle enemmän haittaa. Huijausohjelman täysversiolla, jota ohjelma kehottaa ostamaan skannauksen jälkeen, yritetään rahastaa käyttäjiä, jotka asensivat huijausohjelman ilmaisversion koneelleen. Valitettavan moni käyttäjä erehtyy ostamaan täysversion ja toteaa liian myöhään tulleensa huijatuksi.

Kuva 7. Esimerkki SpySheriff -huijausohjelman mainoksesta (Symantec 2013).

Paras keino välttyä huijausohjelmilta on pysyä kaukana epäluotettavilta sivuilta. Jos näytölle kuitenkin ilmestyy huijausohjelman mainos, käyttäjän tulee pysyä tyynenä, sulkea ilmoitus ja skannata kone luotettavalla virustorjuntasovelluksella. Jos sama ilmoitus alkaa ilmestyä säännöllisin väliajoin, esimerkiksi koneen käynnistymisen yhteydessä tai Internet selaimen avaamisen yhteydessä, eikä

skannaus löytänyt koneelta mitään haittaohjelmaan viittaavaa, scarewaren poistoon soveltuvat ohjeet ja työkalut löytyvät hakukoneella.

6.8 Ransomware

Ransomware on Scareware–haittaohjelmaa kehittyneempi mukaelma, joka nimensä mukaisesti kaappaa koneen haltuunsa lunnaita vastaan. Ransomware –haittaohjelmat voivat kaapata koneen eri tavoin. Ransomware–haittaohjelma kaappaa koneen tiedot esimerkiksi joko salaamalla käyttäjän tiedostot siten, ettei käyttäjä voi käsitellä salattuja tiedostoja, tai lukitsemalla koneelta kaikki muut tiedostot ja sovellukset paitsi internet-selaimen, jota uhrin tulisi käyttää lunnaiden maksamiseen.

Kaapattua konetta on hyvin vaikea pelastaa menettämättä tiedostoja. Useimmiten ainoaksi vaihtoehdoksi jää koneen käyttöjärjestelmän ja ohjelmien uudelleenasennus. Ransomware on pohjimmiltaan Scareware–haittaohjelma, joten molemmilta haittaohjelmilta välttyy noudattamalla samoja ohjeita.

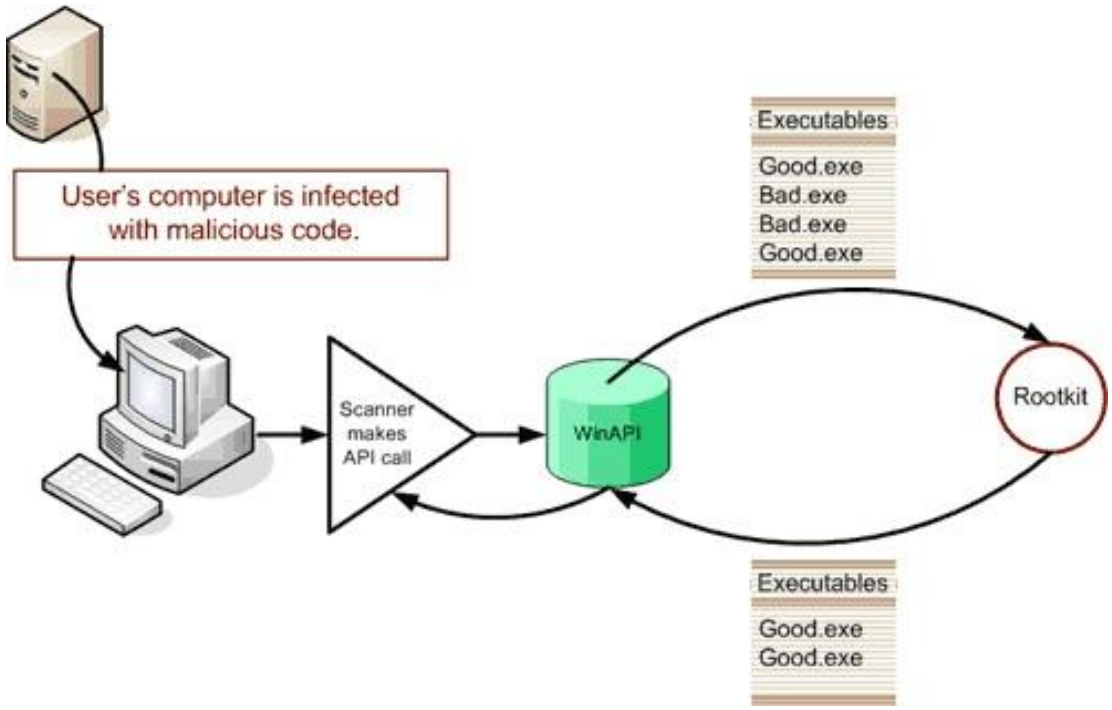
Vaikutus CIA-kolmioon: Scarewaren ja ransomwaren aiheuttamat vahingot vaihtelevat haittaohjelmien toimintatavan mukaan. Jos käyttäjä erehtyy ostamaan scarewaren täysiversion, hänen yhteystietonsa sekä pankkitietonsa päätyvät rikollisille. Tämä vaarantaa tietojen luottamuksellisuuden, sillä kyseessä on käyttäjän kannalta arkaluonteista tai henkilökohtaista tietoa. Ransomware, joka kaappaa koneen, vaarantaa tietojen saatavuuden. Jos ransomwaresta ei pääse eroon muutoin kuin käyttöjärjestelmän uudelleenasennuksella, joitakin tiedostoja saatetaan menettää uudelleenasennuksen yhteydessä.

6.9 Rootkit

Rootkit–haittaohjelman päätarkoituksena on piilottaa koneella käynnissä olevia prosesseja ja sovelluksia (Kuva 8), jotka käyttäjä muutoin löytäisi esimerkiksi virustorjuntasovelluksella. Rootkit asentaa itsensä koneen käyttöjärjestelmän

juureen, jonka vuoksi rootkit–haittaohjelma aktivoituu joka kerta, kun kone käynnistetään. (ZSecurity 2013.)

Kun murtautuja on asentanut koneelle rootkit–haittaohjelman, hän voi salata koneelle muodostettuja yhteydenottoja sekä käyttöjärjestelmän taustalla toimivia prosesseja. Rootkitin ansiosta murtautuja pystyy kontrolloimaan, mitä koneen käyttäjä näkee koneen toiminnasta ja mitä ei. Käytännössä tätä hyödynnetään etäyhteyksien muodostamiseen sekä tietoturvasovellusten muokkaamiseen esimerkiksi siten, että virustorjuntaohjelmat eivät löydä haittaohjelmia ja palomuuri sallii kaiken liikenteen, tai tietoturvasovelluksien poistamiseen käyttäjän huomaamatta. (ZSecurity 2013.)



Kuva 8. Esimerkki Rootkit -haittaohjelman toiminnasta (GR INFOLAB 2013).

Rootkit on kenties vaarallisin haittaohjelmatyyppi. Sitä on erittäin vaikea havaita ja käytännössä lähes mahdotonta poistaa koneelta tyhjentämättä koko koneen kiintolevyä. Paras keino välttyä rootkitin haitoilta on estää rootkitin asentuminen koneelle samoin tavoin kuin muidenkin haittaohjelmien estäminen. Käyttäjän tulee huolehtia tietoturvan ja käyttöjärjestelmän päivityksistä. Lisäksi käyttäjän tulisi aina suhtautua varauksella netistä ladattavia ohjelmia kohtaan.

Vaikutus CIA-kolmioon: Rootkit kätkee koneelle muodostettuja yhteyksiä sekä käynnissä olevia prosesseja. Rootkit pystyy poistamaan jäljet tartunnasta sekä kätkemään koneella olevia muita haittaohjelmia. Tämä itsessään tarkoittaa tietojen eheyden vaarantamista. Kätketyt yhteydet antavat murtautujille vapaan pääsyn ilman autentikointia koneen tiedostoihin, joka puolestaan vaarantaa tietojen luottamuksellisuuden.

Rootkit ei suoranaisesti vaaranna tietojen saatavuutta. Koneen tiedostojen poistaminen sekä muokkaaminen ovat näkyviä toimenpiteitä ja rootkitin tarkoitus on pysytellä näkymättömänä, mutta rootkit helpottaa muiden haittaohjelmien asentamista, mitkä puolestaan voivat vaarantaa tietojen saatavuuden.

7 VARASTETTUJEN TIETOJEN HYÖDYNTÄMINEN

Tietojen varastaminen ei ole uusi ilmiö. Yritykset ovat jo kauan sitten todenneet miten merkittävän edun yritysvakoilulla voidaan saavuttaa kilpailijoihin nähden. Internetin yleistymisen myötä potentiaalisten vakoilukohteiden määrä on moninkertaistunut siitä, mitä se oli 1990-luvun alussa. Valtion virastojen ja laitosten sekä yritysten lisäksi myös peruskäyttäjät voivat joutua tietovarkauden kohteiksi. Toisin sanoen tietovarkaudet koskevat tänä päivänä kaikkia niitä henkilöitä, jotka käyttävät Internetin palveluita säännöllisesti. Siksi onkin tärkeää tietää, mitä seurauksia huonosti toteutetulla tietoturvalla ja omalla huolimattomuudella voi olla.

7.1 Maksukortti

Varastettuja maksukorttitietoja on vaikea käyttää jäämättä kiinni, mutta ovelat rikolliset tietävät, millä keinoilla kiinnijäämisen riski voidaan mitätöidä lähes kokonaan. Verkkohuutokaupat, kuten Huuto.net, ovat erinomaisia paikkoja varastettujen maksukorttitietojen hyödyntämiseen.

> ”Varas voi asettaa verkkohuutokauppaan myyntiin esimerkiksi upouuden television, jota hänellä ei todellisuudessa ole. Kun uhri tarttuu syöttiin ja haluaa ostaa laitteen, varas lupaa toimittaa television pikimmiten. Uhri ei osaa pelätä huijausta, sillä hän saa luvan maksaa laitteen vasta kun on nähnyt, että se on todella kunnossa. Varas käyttää anastettuja luottokorttitietoja ostaessaan toisesta verkkokaupasta television, jonka hän tilaa huutokauppauhrin osoitteeseen. Kun uhri vastaanottaa television, hän ei osaa epäillä mitään, vaan maksaa kiltisti varkaalle. Varas pyytää maksun anonyymillä rahansiirtopalvelulla, kuten Western Unionilla, jolloin hänestä ei jää juuri jälkiä. Kun huijaus paljastuu, poliisit kolkuttavat ensimmäiseksi television ostaneen uhrin ovea. Todellisen huijarin jäljittäminen osoittautuu äärimmäisen mutkikkaaksi” (Vanhala 2012).

Tästä syystä nettihuutokaupoissa asioidessa kannattaa olla tarkkana. Käyttäjätunnuksien tekeminen on helppoa ja nopeaa, yksi huijari voi tehdä lyhyessä ajassa useita käyttäjätunnuksia kaupantekoa tai hyvän palautteen antamiseen. Tämän vuoksi nettihuutokauppojen asiakkaiden kannattaa pyrkiä asioimaan sellaisten kaupittelijoiden kanssa, jotka ovat saaneet hyvää palautetta monelta

eri käyttäjältä ja ovat olleet palvelun käyttäjiä pitkään. Nettihuutokaupassa ei kannata olla liian luottavainen, eikä ainakaan tehdä suuria kauppoja juuri hiljattain rekisteröityneiden käyttäjien kanssa.

7.2 Henkilötiedot

Varastettuja henkilötietoja käytetään identiteettivarkauksiin. Identiteettivarkaus antaa varkaalle mahdollisuuksia mm. henkilöllisyystodistusten kuten ajokortin tai passin väärentämiseen, puhelinliittymien avaamiseen, tavaroiden tilaamiseen tai kulkuvälineiden vuokraamiseen käyttäen uhrin tietoja. Tämän seurauksena maksut lankeavat uhrille ja varas saa tilaamansa tuotteet tai palvelut itselleen. Väärennetyillä tiedoilla avatuilla liittymillä voi tilata melkein mitä vain, ja muutamassa viikossa identiteettivaras saattaa tehdä jopa kymmenien tuhansien eurojen petokset. (Åström-Kupsanen 2012).

Yleisin tapa joutua identiteettivarkauden uhriksi on passin tai ajokortin hukkaaminen, joko katoamisen tai taskuvarkauden johdosta julkisella paikalla. Nettirikollisilla puolestaan on tapana kerätä tarvitsemansa tiedot uhreilta haittaohjelmien tai phishing-viestien avulla.

Uhri saa tietää identiteettivarkaudesta vasta, kun ensimmäiset laskut jäävät maksamatta, joten varkaalla on paljon aikaa käyttää varastettuja tietoja ennen kuin uhri ehtii reagoimaan tilanteeseen. Henkilökortin katoamisen huomaa nopeasti, mutta netin välityksellä tapahtuvaa tiedonkeräämistä on vaikeampi havaita, eivätkä uhrit aina edes tiedä paljastaneensa henkilötietojaan rikollisille.

Jos uhrin tietoja päätyy rikollisille, uhri voi välttää vastuun varkaan aiheuttamasta laskusta, jos uhri pystyy todistamaan, että joku muu on laskujen takana. Useimmissa tapauksissa maksukorttien kuolettaminen ja poliisille tehty ilmoitus ennen ensimmäistä maksutapahtumaa ovat riittäviä todisteita. Lisäksi uhri voi hankkia luottotietoihinsa Oma Luottokielto –merkinnän, jonka avulla voidaan estää varastettujen henkilötietojen käyttö esim. luotonhaussa tai puhelinliittymien avaamiseen. (Åström-Kupsanen 2012.)

7.3 Sähköposti ja muut käyttäjätunnukset

Käyttäjätunnuksien varastamisesta saatava hyöty riippuu pitkälti siitä, minkä palvelun käyttäjätunnukset ovat kyseessä. Keskustelufoorumin käyttäjätunnuksien päätyminen vääriin käsiin ei ole kovin katastrofaalista, mutta sähköpostin tai verkkopankin tunnuksilla voidaan aiheuttaa suurta vahinkoa. Uutta käyttäjätunnusta tehdessä, oli kyseessä mikä tahansa verkkosivu tai palvelu, käyttäjältä kysytään sähköpostiosoitetta, johon voidaan lähettää palvelun tunnuksen salasanan nollauksen vahvistus siltä varalta, että käyttäjä unohtaa salasanansa, joten sähköpostitunnuksen päätyminen vääriin käsiin voi mahdollistaa useiden käyttäjätunnuksien väärinkäytön.

Sähköpostin liitetiedostot ovat kätevä tapa siirtää tiedostoja työpaikalta kotikoneelle tai kannettavalle, mutta sähköpostia ei suinkaan tulisi käyttää tiedostojen varastoimiseen. Yhdenkin keskenjääneen uloskirjautumisen, hukatun muistilapun johon käyttäjä on kirjoittanut käyttäjätunnuksensa ja salasanansa, tai koneelle asentuneen haittaohjelman seurauksena yrityksen arkaluonteiset tiedostot voivat päätyä rikollisen käsiin, ja työntekijää pidetään vastuussa tietojen vuotamisesta.

Tämän vuoksi on syytä poistaa kyseiset sähköpostit heti, kun liitetiedoston on ladannut koneelle eikä viestiä enää tarvita. Sama sääntö koskee myös Dropbox –pilvipalvelua, johon käyttäjät voivat lisätä omia tiedostojaan ja ladata kyseiset tiedostot muille koneille. Toisin sanoen Dropbox on ikään kuin Internetin välityksellä toimiva USB-muistitikku, joten sitä tulisi käsitellä yhtä huolellisesti kuin USB-muistitikkua.

8 TUNNETTUJA HAKKERIRYHMIÄ JA HAKKEREITA

8.1 The 414s

The 414s tunnetaan parhaiten v. 1983 Sloan-Kettering syöpähoitolaitoksen tietomurrosta. Sama ryhmä sai julkisuutta Los Alamosin kansallisen laboratorion (Los Alamos National Laboratory) sekä Security Pacific Bank –pankin tietomurroista. (The TEXTFILES.COM 2012.)

Ryhmä koostui kuudesta 16-22 –vuotiaista hakkereista, jotka asuivat Milwaukeen alueella. Ryhmän nimi on johdettu Milwaukeen suuntanumerosta 414. Ryhmän puhemieheksi valikoitui tuolloin 17-vuotias Neal Patrick, jonka omien sanojen mukaan ryhmän motivaationa ei ollut aiheuttaa vahinkoa, vaan hakea jännitystä menemällä paikkoihin, joihin ei ollut lupaa mennä ja olla jäämättä kiinni. The 414s–ryhmän kohteina olivat yleensä koneet, jotka käyttivät VMS –käyttöjärjestelmää. Ryhmän jäsenet käyttivät murroissaan halpoja kotikoneita sekä alkeellisia murtometodeja, esim. kokeilivat oletussalasanoja tai helposti arvattavia salasanoja, sekä yleisesti tunnettuja korjaamattomia turva-aukkoja. (The 414s 2012.)

Ryhmän menestys aiheutti suuria huolia turvallisuusasiantuntijoiden keskuudessa. He ymmärsivät, että muut hakkerit voivat jäljitellä heidän metodejaan ja aiheuttaa tahallaan suurta vahinkoa. (The TEXTFILES.COM 2012.)

Sloan-Kettering –tapaus johti The 414s–ryhmän kiinnijäämiseen. Tapaus sai alkunsa, kun ryhmän jäsen Gerald Wondra murtautui laitoksen palvelimelle 3. kesäkuuta ja tuhosi tiedostoja peitelläkseen omat jälkensä. Seuraavien päivien aikana järjestelmään ilmestyi uusia luvattomia käyttäjätunnuksia sekä ohjelmia, jotka kopioivat muiden käyttäjätunnuksien salasanoja antaen murtautujille vapaan pääsyn laitoksen työntekijöiden tiedostoihin. (The TEXTFILES.COM 2012.)

Laitoksen järjestelmävalvoja, Chen Chui, kuitenkin huomasi puuttuvat tiedostot, poisti luvattomat tunnukset sekä jätti tunkeutujalle varoitusviestin, jossa Chui kertoi, mitä seurauksia ja vahinkoja järjestelmän kaatumisesta voi koitua laitokselle. Wondra soitti Chuille ja kertoi vain olleensa utelias ja piti hakkerointia harmittomana hauskanpitona. Chui otti yhteyttä New Yorkin poliisilaitokseen, FBI:hin sekä puhelinlaitoksen viranomaisiin ja jätti pyynnön salakuunnella murtautujan yleisimmin käyttämiä puhelinlinjoja. Tämän toimenpiteen ansiosta viranomaiset pääsivät The 414s–ryhmän jäljille ja saivat ryhmän jäsenet kiinni elokuussa 1983. (THE TEXTFILES.COM 2012.)

26. syyskuuta 1983 Neal Patrick todisti Yhdysvaltain kongressissa, miten helppoa järjestelmiin on murtautua ja esitti keinoja, joilla murtoja voitaisiin jatkossa estää. Samana vuonna kehitettiin kuusi lakiesitystä, joilla kriminalisointiin hakkerointia ja tietokonerikoksia. (The Washington Post 2013.)

The 414s–ryhmästä tuli onnekkaan sattuman kautta tärkeä White hat –hakkeriryhmä. Jos Gerald Wondra ei olisi jäänyt kiinni, Neal Patrick ei todennäköisesti olisi päässyt kongressin eteen todistamaan tietomurtojen vaarallisuudesta. Jos Los Alamosin tietomurron taustalla olisi ollut jokin toinen hakkeriryhmä, seuraukset olisivat voineet olla hyvin vakavia, sillä Los Alamosin laboratorio on Yhdysvaltojen suurimpia ydinaseiden kehittäjiä. (Los Alamos National Laboratory 2012.)

8.2 LulzSec

LulzSec –ryhmä sai alkunsa toukokuussa 2011 ja sai lyhyen ajan sisällä paljon huomiota hyökkäämällä vaativina murtokohteina pidettyihin sivustoihin ja palvelimiin. Ryhmä koostui seitsemästä avainhenkilöstä. Ryhmään saattoi kuulua muitakin jäseniä, mutta LulzSec –ryhmää ollaan pidetty toimettomana ryhmän johtajan ja avainhenkilöiden kiinnijäämisen jälkeen. LulzSec ilmoitti tehneensä tietomurtoja pilailumielessä eikä käyttänyt varastamiaan tietojaan ansaitakseen rahaa. Ryhmän tarkoituksena oli lähinnä osoittaa, että alkeellisillakin murtome-

netelmillä pääsee vielä nykypäivänä useisiin palvelimiin ja verkkoihin. Toimintatapojensa vuoksi LulzSec leimattiin Grey Hat -hakkeriryhmäksi. (Leyden 2013.)

Ryhmän lyhyeksi jäänyt ura sai alkunsa, kun ryhmä hyökkäsi Fox -televisioyhtiön nettisivuille toukokuussa 2011 ja vei arviolta 73 000 X Factor –ohjelman kilpailijoiden nimet. Toukokuun 15. päivä LulzSec julkaisi Isossa-Britanniassa sijaitsevien 3100 käteisautomaatin tapahtumalokit. LulzSec sai maailmanlaajuista huomiota onnistuttuaan hakkeroimaan Yhdysvalloissa toimivan Public Broadcast Services (PBS) –televisioyhtiön verkkosivut. Hyökkäyksen yhteydessä LulzSec varasti käyttäjien tietoja sekä laati pilailumielessä valheellisia uutisia. (Li 2011.)

Kesäkuussa 2011 LulzSec teki lukuisia murtoja pelialan yrityksiä, pelialan verkkosivuja sekä viranomaisten ja valtioiden palvelimia kohtaan (Bright 2011). Ainoastaan CIA:n ja pelialan verkkosivut joutuivat DDos –hyökkäyksien kohteeksi (Nakashima 2011). Muut hyökkäyksen kohteina olleet saivat palautetta LulzSecin hakkereilta järjestelmien haavoittuvuuksista (BBC News 2013).

LulzSecin johtaja Hector Xavier Monsegur, nimimerkki Sabu, pidätettiin kesäkuussa 2011. Elokuun 15. päivä Hector tunnusti syyllistyneen hakkerointiin ja suostui tekemään yhteistyötä FBI:n kanssa. Seuraavan seitsemän kuukauden ajan Hector auttoi FBI:tä jäljittämään muut LulzSecin jäsenet ja ilmiantoi heidät viranomaisille. (Winter 2012.) Maaliskuuhun 2012 mennessä suurin osa LulzSecin jäsenistä oli pidätetty ja tuomittu, viimeinen pidätys tehtiin 24. huhtikuuta 2013 (ABC News 2013).

LulzSec –ryhmästä ei ole kuultu mitään viimeisten pidätysten jälkeen.

8.3 Anonymous

Anonymous –ryhmä tunnetaan monista suuryrityksiin sekä valtioiden laitoksien verkkosivuihin ja palvelimiin kohdistuneista hyökkäyksistä. Murtokohteiden listalta löytyy mm. Sony ja NASA. Anonymous on haktivismiryhmä, joka ei tavoittele taloudellista hyötyä, vaan haluaa saada muutoksia aikaan joko kannatta-

malla sananvapautta edistäviä ryhmiä tai protestoimalla sananvapautta sekä yksittäisten henkilöiden vapauksia rajoittavia ja yksittäisten henkilöiden yksityisyyttä loukkaavia hankkeita. (Coleman 2011.)

Anonymousin jäsenien tiedetään osallistuneen myös tavanomaisiin mielenosoituksiin pitäen kasvoillaan Anonymous –ryhmän symbolia, Guy Fawkes-maskia, joka tuli tunnetuksi vuonna 2005 julkaistun elokuvan *V niin kuin verikosto* (eng. *V for Vendetta*) myötä. (Waiters 2011.)

Kuva 9. Anonymous -ryhmän logo (Olson 2013).

Anonymous –ryhmällä ei ole johtajaa eikä hallintoelintä (Kuva 9), eikä Anonymousin jäseneksi haeta. Riittää, että henkilö haluaa kannattaa Anonymouksen toimintaa. Kuka tahansa saa aloittaa projektin, ainoa edellytys tapahtuman tai operaation järjestymiselle on, saako hanke tarpeeksi kannatusta ja näkyvyyttä. (Coleman 2011.)

Anonymous –ryhmän tekoihin lukeutuvat mm. seuraavat tapahtumat:

Useat rahalaitokset, mm. Visa, Mastercard, PayPal, kieltäytyivät vuonna 2010 välittämästä WikiLeaksille suunnattuja lahjoituksia, johon Anonymous reagoi tekemällä palvelunestohyökkäyksiä rahalaitoksia vastaan. Elokuussa 2010

Anonymous otti kohteekseen useita yhdysvaltalaisia ja iso-britannialaisia sivustoja Julian Assangeen liittyvien toimien vuoksi. (Halliday & Arthur 2010.)

Vuonna 2012 marraskuun 17. päivä Anonymous protestoi Gazan kaistaan suunnattuja iskuja murtautumalla satoihin tietokantoihin, mm. Bank Jerusalemin ja Israelin ulkoministeriön tietokantoihin, joiden yhteydessä Anonymous vei tuhansien Israelin tukijoiden henkilötietoja. Lisäksi Anonymous kaatoi yli 650 sivustoa. (Protalinski 2012.)

Kaksi viikkoa myöhemmin Syyrian Internet yhteys katkaistiin kansannousun vuoksi. Anonymous vastasi maan Internet pimentoon julistamalla sodan Syyrian hallitusta vastaan ja vannoi sulkevansa kaikki Syyrian hallituksen sivustot. (Bennett-Smith 2012.)

8.4 WikiLeaks

WikiLeaks on internetsivusto, joka antaa yksityishenkilöille mahdollisuuden vuotaa salaisiksi luokiteltuja poliittisia tai kaupallisia dokumentteja ilman kiinnijäämisen pelkoa (Williamson 2007). Monien maiden hallitukset ovat kritisoineet sivustoa kansallisen turvallisuuden vaarantamisesta sekä muista tietovuotojen mahdollisista seuraamuksista. Toisaalta monet muut tahot ovat antaneet positiivista palautetta WikiLeaksin paljastettua lukuisia laittomuuksia sekä epäilyttäviä tekoja, joita valtiot ovat yrittäneet pitää kansalta salassa.

WikiLeaksissa julkaistuja asiakirjoja:

Sivustolla julkaistiin 7. marraskuuta 2007 Guantanamo Bayn vankileirin Yhdysvaltain armeijan henkilöstön toimintaohjeisto vuodelta 2003. Kyseinen dokumentti kantoi nimeä Standard Operating Procedures for Camp Delta. Ohjeistossa paljastettiin, että eräät vangit on sijoitettu alueille, joille ei päästetä Punaisen Ristin kansainvälisen komitean tarkkailijoita. 3. joulukuuta sivustolla julkaistiin myös vuoden 2004 versio ja kahden version välisten muutosten vertailu (Sutton, 2007).

Huhtikuussa 2010 sivusto julkaisi videon, jolla Yhdysvaltain armeijan helikopteri ampuu Bagdadissa siviilejä, mukaan lukien Reutersin valokuvaajan Namir Noor-Eldeenin (Bumiller 2010).

8.5 Albert Gonzalez

Albert Gonzalez, synt. 1981, tunnetaan parhaiten TJX Companyn ja Heartland Payment Systems –yritysten tietomurroista. Gonzalezin kerrotaan tehneen ensimmäisen tietomurtonsa hänen ollessaan yläasteella 1990 –luvulla, jolloin hän pääsi Intian hallituksen ylläpitämälle verkkosivulle. Hän sai murrostaan varoituksen ja kehotuksen pysytellä poissa tietokoneilta puolen vuoden ajan. (Faustus 2010.)

19 –vuotiaana Gonzalez perusti hakkeriryhmän ShadowCrew, joka varasti luotto- ja maksukorttitietoja ja myi niitä eteenpäin. Lisäksi ShadowCrew väärensi huutokaupattavia asiakirjoja sekä tarjosi oppaita luottokorttien salausten purkamiseen. Gonzalez pidätettiin huhtikuussa 2003 jäätyään kiinni 15 väärennetyn luottokortin omistamisesta. Hän kuitenkin välttyi vankilalta ilmiannettuaan 19 ShadowCrew –ryhmän jäsentä. Pidätyksen jälkeen hän suostui tekemään yhteistyötä viranomaisten kanssa ja ryhtyi poliisin tiedonantajaksi. (Albert Gonzalez 2013.)

Albert Gonzalez jäi kiinni uudestaan 7.5.2008 TJX Companyn ja Heartland Payment Systems –tietomurtojen jälkeen. Albert Gonzalez ja hänen ryhmänsä olivat ottaneet kohteekseen paikallisen Dave & Buster’s –ravintolan. He onnistuivat hakkeroimaan yhden myyntipisteen, joka keräsi tuhansia luottokorttinumeroita.

Heidän hakkerointimenetelmässään oli kuitenkin yksi puute. Hakkerointi piti aloittaa alusta aina, kun myyntijärjestelmä oli sammutettu ja käynnistetty uudelleen. Tämän takia Gonzalezin ryhmä kävi samassa ravintolassa useita kertoja varmistaakseen, että hakkeroitu laite keräsi numeroita. Gonzalezin aiemmin tekemät rikokset, jatkuvat vierailut samassa ravintolassa ja epäilyttävä käytös johtivat hänen pidätykseensä. 25. Maaliskuuta 2010 Gonzalez sai 20 vuoden

vankeustuomion TJX ja Heartland Payment Systems –tietomurroista, lisäksi hänelle määrättiin 25,000 dollarin edestä sakkoja. (Faustus 2010.)

8.6 Kevin Mitnick

Kevin Mitnick, synt. 1963, on yksi kaikkien aikojen tunnetuimpia hakkereita. Hän aloitti uransa Black Hat –hakkerina ja on jatkanut toimintaansa kiinnijäämisensä jälkeen White Hat –hakkerina.

Mitnick otti ensiaskeleensa rikollisurallaan vuonna 1975 hänen ollessaan 12-vuotias, jolloin hän selvitti, mistä hän saisi hankittua Los Angelesin bussiyhtiön kuljettajien käyttämän leimasimen ja käytti hankkimaansa leimasinta omien bussilippujen väärentämiseen. Tuohon aikaan bussinkuljettajat heittivät käyttämättömät tyhjät liput roskiin työvuoronsa päätteeksi, joten leimaamattomia lippuja oli helppo löytää. (Gots 2011.)

Vuonna 1979 16-vuotias Mitnick tapasi koulussaan hakkeriryhmän ja halusi päästä ryhmän jäseneksi. Ryhmä antoi hänelle haasteeksi murtautua DEC -yhtiön The Ark–tietokonejärjestelmään. Ryhmä oli saanut käsiinsä yhtiön käyttämän dial-up numeron, joita vanhanaikaiset modeemiyhteydet käyttivät internet-yhteyksien muodostamiseen, mutta järjestelmään pääsy vaati numeron lisäksi käyttäjätunnuksen ja salasanan. Mitnick soitti DEC –yhtiön järjestelmänvalvojalle ja esitti olevansa Anton Chernoff, yksi The Ark–järjestelmän johtavista kehittäjistä ja kertoi unohtaneen salasanansa. Viisi minuuttia myöhemmin Mitnickillä oli vapaa pääsy yhtiön suojattuun järjestelmään. (Greene 2003.)

Päästyään DEC –yhtiön järjestelmään Mitnick kopioi yrityksen kehittämiä sovelluksia, jonka seurauksena hän sai vuoden vankeustuomion ja kolmen vuoden ehdonalaisen jälkeenpäin vuonna 1988. Ehdonalaisen loppupuolella Mitnick murtautui Pacific Bell –puhelinyhtiön ääniviestien tietokoneille. Tämän seurauksena Mitnick sai pidätysmääräyksen ja hän ryhtyi pakolaiseksi seuraavaksi kahdeksi ja puoleksi vuodeksi. (Greene 2003.)

Kevin Mitnick pidätettiin 15.2.1995 ja hänelle määrättiin viiden vuoden vankeustuomio. Vapauduttuaan vankilasta 21.1.2000 Mitnick pääsi tarkkailunalaiseen vapauteen kolmeksi vuodeksi. (Kahney 2003.)

Mitnick ryhtyi vankeutensa jälkeen White Hat –hakkeriksi ja perusti Mitnick Security Consulting LLC –yrityksen. (Mitnick Security Consulting 2013.)

9 TUNNETTUJA MURTOMETODEJA

9.1 Tietokoneen etähallinta ja tiedostojen varastaminen kohdekoneelta

Tietokoneen etähallinta tarkoittaa nimensä mukaisesti tietokoneen hallitsemista, yleensä tietokoneen käyttäjän tietämättä, etäyhteydellä. Murtautuja voi hallita konetta joko manuaalisesti tai käyttää botteja, jotka suorittavat koneelle lähetettyjä käskyjä. Etäyhteyden ansiosta murtautuja pääsee tarkastelemaan koneen tiedostoja sekä pystyy lataamaan tiedostoja suoraan kohdekoneelta omaan käyttöönsä.

Konetta voidaan hyödyntää rikollistoimintaan vaikka koneella ei olisikaan arvokkaita tietoja. Kone voidaan liittää osaksi bottiverkkoa. Bottiverkkojen ylläpitäjät yleensä osaavat peitellä jälkensä siten, ettei heidän voida epäillä olleen tekemisissä bottiverkon kanssa millään lailla, kun taas bottiverkon koneet ovat paljon näkyvämpiä. Tästä syystä bottiverkkoon liitettyjen koneiden omistajia pidetään korvausvelvollisina, jos bottiverkkoa käytetään vahingontekoon.

Tietokoneen etähallinta edellyttää seuraavien ehtojen täyttymisen: Koneen on oltava yhteydessä Internetiin ja koneella on oltava portteja avoinna, joiden kautta muodostetaan etäyhteys. Avoimien porttien selvittämistä varten on olemassa porttiskannaussovelluksia, joiden laillisuudesta ei olla päästy yksimielisyyteen. Vaikka porttiskannereita käytetään usein tietomurtojen apuvälineinä, monien yritysten järjestelmänvalvojat ja tietoturvavastaavat käyttävät porttiskannereita verkon haavoittuvuuksien paikantamiseen.

Haittaohjelmat, kuten virukset ja troijalaiset, voivat avata koneen portteja käyttäjän tietämättä. Tästä syystä saastunut kone on alttiimpi tietomurroille kuin oikeaoppisesti suojattu kone.

Kohdekoneen IP osoitteen on oltava tiedossa, jotta porttiskannaus voidaan suorittaa. Yleensä rikolliset käyttävät IP osoitteen selvittämiseen phishing–viestiä,

joka postittaa uhrin IP-osoitteen ennalta määrättyyn sähköpostiosoitteeseen, jos uhri klikkaa viestin linkkiä.

Viestintäsovelluksiakin voidaan käyttää IP-osoitteen selvittämiseen: Skypessä havaittiin tietoturvariski, joka mahdollisti IP-osoitteen jäljittämisen. Kyseinen riski havaittiin marraskuussa 2010. Tietoturvariskin havainnut henkilö teki uusintakokeen huhtikuussa 2012, eikä ongelmaa oltu vielä tuolloin korjattu. (Schectman 2012.)

9.2 Käyttäjän tietojen ja tunnuksien varastaminen

Haittaohjelmia ja botteja voidaan käyttää tietojen keräämiseen ja lähettämiseen ennalta määrättyyn kohteeseen. Salasanojen ja käyttäjätunnuksien selvittämiseen on ollut jo pitkään käytössä keylogger–sovelluksia, jotka tallentavat kaikki näppäimistönpainallukset tekstitiedostoon ja lähettävät kyseisen tiedoston rikollisille.

Keyloggereissa on kuitenkin omat puutteensa. Vaikka keyloggerilla saa selvitettyä, mitä käyttäjä on kirjoittanut Internet-selaimen osoitepalkkiin sekä sivun käyttäjätunnuksen ja salasanan, keylogger kirjaa ylös kaikki painallukset, kirjoitusvirheet mukaan lukien, juuri siinä järjestyksessä kuin käyttäjä syöttää napinpainalluksia koneelle. Toisin sanoen keyloggerin tekstitiedostossa tiedot voivat olla sekavassa järjestyksessä. Jos käyttäjä on syöttänyt koneelle Leikkaa – Liitä –käskyjä, niin keylogger ei kerro Leikkaa – Liitä –käskyillä täytettyjen tekstikenttien sisältöä. Lisäksi keylogger ei kirjaa, mitä käyttäjä on valinnut lomakkeen pudotusvalikoista (Kuva 10).

Kuva 10. Esimerkki lomakkeesta. Huomaa pudotusvalikko State (Information Systems Security 2013).

Form Grabbing–menetelmä, eli lomaketietojen kaappaaminen, on pitkälti korvannut keylogger–ohjelmat Internet sivustojen käyttäjätunnusten ja salasanojen selvittämisessä. Keyloggeriin verrattuna Form Grabbing kertoo tarkalleen, mitä käyttäjä on syöttänyt mihinkin tekstikenttään, sekä kertoo samalla tekstikentän otsikon. Keyloggeria voidaan kuitenkin käyttää myös muiden sovellusten, esimerkiksi yrityksen tietokantajärjestelmän, käyttäjätunnusten ja salasanojen varastamiseen.

Suurin ero keyloggerin ja Form Grabbing –menetelmän välillä on, että keylogger kirjaa kaikki painallukset keylogger –ohjelman käynnistymisen jälkeen, mikä yleensä tapahtuu koneen käynnistymisen yhteydessä. Form Grabbing puolestaan keskittyy pelkästään Internet-selaimessa täytettyihin lomakkeisiin ja lähettää tiedot eteenpäin vasta, kun käyttäjä on klikannut lomakkeesta Lähetä tiedot –painiketta. Lomakkeen tiedot menevät ensin rikolliselle ja sitten vasta Internet-sivun palvelimelle. Form Grabber asentaa itsensä internet-selaimen liitännäiseksi, jonka vuoksi suojattu yhteys, esimerkiksi HTTPS, ei suojaa Form Grabbing –metodilta (Information Systems Security 2013).

9.3 Verkkoon kohdistetut hyökkäykset

Yksittäisten koneiden lisäksi hyökkäyksiä voidaan kohdistaa myös koko verkkoa vastaan.

Palvelunestohyökkäys, Denial of Service, on yleisin verkkoon kohdistettu hyökkäys. Nimensä mukaisesti hyökkäyksen tavoitteena on ruuhkauttaa verkon palvelimia ja laitteita siten, että palvelun käyttäjien palvelupyynnöt eivät kulje palvelimille asti.

Palvelimilla ja verkon laitteilla, kuten reitittimillä ja kytkimillä, on käytössään rajallinen määrä käyttömuistia, johon palvelupyynnöt jäävät jonoon, jos laite vielä käsittelee aiempaa palvelupyyntöä. Jos laitteelle lähetetään riittävän pitkään palvelupyyntöjä nopeammin kuin mitä kyseinen laite pystyy käsittelemään palvelupyyntöjä, laitteen käyttömuisti loppuu kesken ja laite menee jumiin. Jos palvelun käyttäjän ja palvelimen välillä ei ole yhtäkään vapaata laitetta käsittelemässä käyttäjän lähettämää palvelupyyntöä, käyttäjän palvelupyyntö ei mene palvelimelle asti.

Verkon ruuhkauttamisen kannalta on tärkeää, että kaikki palvelupyynnöt saapuvat laitteille lyhyen ajan sisällä. Tämän vuoksi palvelunestohyökkäyksissä käytetään usein apuna bottiverkkoa, mitä suurempi verkko ja mitä enemmän laitteita, sitä enemmän verkkoliikennettä tarvitaan verkon ruuhkauttamiseen. Laajasta DoS –hyökkäyksestä käytetään nimitystä DDoS –hyökkäys, eli Distributed Denial of Service.

Uudempi ilmiö verkkoon kohdistetuista hyökkäyksistä ovat Stuxnetin kaltaiset haittaohjelmat. Suljettujen verkkojen, jotka eivät ole kytköksissä Internetiin, oletetaan olevan täysin turvassa haittaohjelmilta ja hakkereilta, jonka takia Stuxnetin kaltaisia haittaohjelmia ei ole osattu huomioida verkkojen suunnitteluvaiheessa. Jo ennen Stuxnetin havaitsemista USA:n valtion alaisuudessa toimiva Department of Homeland Security –yhtiö on tunnustanut olevansa tietoinen Yhdysvaltojen sähköverkon huonosta turvallisuudesta. (Holland & Mikkelsen 2009.)

Vaikka mediassa ei vielä ole raportoitu sähköverkkoihin kohdistetuista hyökkäyksistä, on hyvin todennäköistä, että tämänkaltaisia tietomurtoja tullaan näkemään tulevaisuudessa. Sähköverkosta saattaa tulla jopa houkuttelevampi kohde kuin yhdestäkään maailman laboratorion ja tiedustelupalvelun verkosta. Tämän vuoksi sähköverkkojen tietoturvasta tulisi huolehtia jo hyvissä ajoin ennen kuin ensimmäisistä sähköverkkojen tietomurroista raportoidaan mediassa.

Shodan –skanneri on myös saanut huomiota mediassa. Shodan on pilvipalveluna toimiva porttiskanneri, joka on kaikkien saatavilla (SHODAN 2013). Shodan-skanneria voisi äkkiseltään luulla pelkästään työkaluksi, jota käytetään tietomurron valmisteluksi tai pohjatyöksi. On kuitenkin syytä muistaa, että yritysten tietoturvasta vastaavat henkilöt käyttävät samoja työkaluja järjestelmän haavoittuvuuksien paikantamiseen. Black Hat –hakkerit käyttävät skannereita murtokohteiden tutkimiseen, mutta on tärkeää huomioida, että Shodan on vain yksi skanneri monien joukossa. Black Hat –hakkerit ovat löytäneet haavoittuvuuksia huonosti suojatuista tietoverkoista jo kauan ennen Shodan –skannerin olemassaoloa.

Shodan –skanneria pidetään erityisen vaarallisena siksi, koska se osaa paikallistaa heikosti suojattuja laitteita ympäri maailmaa, myös sellaiset laitteet, jotka on kytketty internetiin ilman näkyvää syytä. Vuonna 2012 pidetyn Defcon -konferenssin luennoitsija Dan Tentler esitti yleisölleen, mitä hän oli löytänyt Shodan –skannerin ja internetiin kytkettyjen laitteiden heikkojen suojauksien ansiosta. Listalta löytyi muun muassa erään USA:n kaupungin liikennevalojen hallintajärjestelmä, Ranskassa sijaitsevan sähkölaitoksen turbiinien hallintajärjestelmä, yrityksen valvontakameroiden hallintajärjestelmä sekä vedenlämmittimien hallintajärjestelmä. Kaikkiin järjestelmiin pääsi käsiksi joko ilman autentikointia tai käyttämällä järjestelmien oletussalasanoja. (Goldman 2013.)

Näiden laitteiden haavoittuvuudet ovat olleet olemassa jo vuosia, mutta haavoittuvuudet ovat tulleet laajalti tietoon vasta Shodan –skannerin myötä. Monet tietoturva-asiantuntijat toivovat, että Shodan –skannerin myötä yritykset ja yksit-

täishenkilöt kiinnittäisivät enemmän huomiota internetiin kytkettäviin järjestelmiin ja laitteisiin.

10 TIETOMURROILTA SUOJAUTUMINEN

10.1 Tietomurtojen ennaltaehkäisy

Tietomurtojen vahingoilta välttyy parhaiten pitämällä huolen siitä, ettei tietokoneessa ole haavoittuvuuksia, joita rikolliset voivat käyttää hyödykseen. Jos mediassa raportoidaan tietomurrosta, joka on kohdistunut yhteen tai useampaan käyttäjän hyödyntämään verkkopalveluun, käyttäjän on syytä reagoida tapahtumaan saman tien ja vaihtaa palvelun salasana sekä varmistaa, että käyttäjän oman koneen tietoturva on ajan tasalla.

Virustorjunta ja palomuurit

Tietomurtojen pahimmat vahingot voidaan välttää pitämällä huolta koneen palomuurin ja virustorjunnan päivityksistä ja tietokoneen oikeaoppisella käytöllä. Ajantasainen palomuuri suodattaa koneelle suunnattua tietoliikennettä ja täten estää koneelle kohdistuvia murtoyrityksiä, kun taas virustorjunta tarkkailee koneen tiedostoja sekä ilmoittaa koneen käyttäjälle, jos koneella on havaittu haittaohjelmia tai jos virustorjunta on poistanut koneelta haittaohjelmia.

Toisinaan virustorjunta- ja palomuurisovellukset antavat vääriä hälytyksiä. Kukin sovellus käyttää omia tunnistetietojaan epäilyttävien tiedostojen ja yhteyksien tunnistamisessa. Tästä syystä useamman virustorjuntasovelluksen sekä haittaohjelmien poistoon tarkoitettujen sovellusten asennus ei välttämättä ole huono ajatus. Sovellus B saattaa löytää koneelta haittaohjelmia, joita sovellus A ei löytänyt. Kannattaa kuitenkin pitää mielessä, että käyttää yhden sovelluksen tarkastustoimintoa kerrallaan. Usean sovelluksen yhtäaikainen tarkastus hidastaa konetta tarpeettomasti ja päällekkäiset tarkastukset sotkevat toisiaan, joten kumpikaan tarkastus ei toimi kunnolla.

Samasta syystä usean palomuurisovelluksen yhtäaikaista käyttöä samalla koneella ei suositella. Kahdesta palomuurista saatava lisäturva on lähes olematon

ja tietoliikenne hidastuu huomattavasti, jos sen täytyy kulkea usean palomuurin lävitse. Pahimmillaan tietoliikenne jää kahden palomuurin väliin ja täten rajoittaa tiedonsiirtoa ja Internet-selaimen käyttöä turhaan.

Salasana

Salasanojen yleissääntö ”helppo muistaa, mutta vaikea arvata” saattaa kuulostaa itsestään selvältä, mutta silti monet käyttäjät laativat liian heikkoja salasanoja. Salasanojen murtamiseen tarkoitetut sovellukset voidaan jakaa kahteen eri luokkaan: sanakirjamurto, dictionary crack, ja raaka voima –murto, brute force crack.

Sanakirjamurto toimii nimensä mukaisesti siten, että sovellus kokeilee kaikkia sanakirjaan syötettyjä sanoja kunnes se löytää oikean salasanan. Tämän vuoksi salasanan ei koskaan tulisi olla selkokielinen sana tai nimi, esimerkiksi kissa tai pekka löytyvät todella nopeasti sanakirjamurrolla.

Raaka voima -murto kokeilee järjestelmällisesti kaikkia mahdollisia numeroita ja kirjaimia, isoja ja pieniä, kunnes se löytää oikean salasanan. Sanakirjamurtoon verrattuna raaka voima -murto on hitaampi, mutta varmempi keino salasanan selvittämiseen. Lisäksi raaka voima -murto on paljon näkyvämpi kuin sanakirja –murto, koska lokitietoihin ilmestyy enemmän virheellisiä kirjautumisyrityksiä. Tämän vuoksi raaka voima -murtoa käytetään enemminkin suojattujen kohteiden, kuten WPA-avaimella salattujen langattomien tukiasemien murtamiseen, eikä niinkään käyttäjien salasanojen selvittämiseen.

Käyttäjätunnuksen ja salasanan selvittäminen murto-ohjelmilla on käytännössä harvinaista mutta mahdollista. Siksi on tärkeää tehdä salasanasta niin monimutkainen, että sen selvittäminen murtosovelluksella vaatii paljon aikaa. Vahva salasana koostuu isoista ja pienistä kirjaimista sekä numeroista, esim. paperi ja Paperi ovat todella heikkoja salasanoja, Paperi12 on hieman vahvempi, mutta silti heikko, kun taas salasanaa Pap3r1 ei välttämättä löydy sovelluksen sanakirjasta ja raaka voima -murrolla salasanan selvittäminen kestää huomattavasti pidempään. Kirjaimien korvaaminen numeroilla on kuitenkin laajalti tunnettu

tekniikka, jonka moni murtautuja tietää ennestään. Tämän vuoksi nämä muunnelmat on usein huomioitu murtosovelluksien sanakirjoja laadittaessa. Kahden toisiinsa liittymättömän sanan yhdistely ja numeroiden lisääminen tekee salasanasta huomattavasti vaikeamman arvattavan.

Toinen salasanoja koskeva yleissääntö on ”Älä koskaan paljasta salasanaasi kenellekään”. Monet rikolliset yrittävät onkia yksittäisten käyttäjien tunnusta ja salasanaa suoraan käyttäjältä joko phishing –viesteillä tai puhelimitse esiintyen järjestelmänvalvojana. Salasana tulisi vaihtaa säännöllisin väliajoin sekä silloin, kun käyttäjä epäilee salasanan paljastuneen. Käyttäjän tulisi aina välttää vanhojen salasanojen kierrättämistä, sekä saman salasanan käyttämistä useassa eri palvelussa.

Turvallinen nettisurffailu

Huolimattomalla koneen käytöllä on useimmiten ikäviä seurauksia. Netistä ladatun tiedoston mukana tulevan haittaohjelman tai huolimattomasta linkkien painelujen johdosta roskapostien postituslistalle päätymisestä käyttäjä saa syyttää vain itseään. Tämän vuoksi käyttäjän tulee aina olla tarkkana, mitä hän on klikkaamassa ja miltä sivuilta hän lataa tiedostoja.

Nettisurffailua koskeva yleissääntö ”Jos jokin näyttää liian hyvältä ollakseen totta, se on liian hyvää ollakseen totta” unohtuu monelta helposti. Kokemattomat koneen käyttäjät saattavat erehtyä klikkaamaan haitalliselle sivulle ohjaavaa linkkiä, jos linkki on naamioitu houkuttelevaksi, esimerkiksi tunnetut ”Onneksi olkoon, olet voittanut lomamatkan! Käy lunastamassa palkintosi” –ponnahdusikkunat. Sivujen sisältöä ei yleensä voi tietää etukäteen, mutta onneksi nykypäivänä virustorjunta- ja palomuurisovellukset reagoivat nopeasti, jos koneelle on tulossa kutsumattomia vieraita.

Tämä ei kuitenkaan tarkoita, että virustorjunnan ja palomuurin päivittäminen itsessään on aukoton suoja haittaohjelmia ja rikollisia vastaan. Käyttäjä on aina vastuussa tietokoneensa toiminnasta. Moniin Internet-selaimiin on saatavilla ilmaisia lisäosia, jotka lisäävät nettisurffailun turvallisuutta.

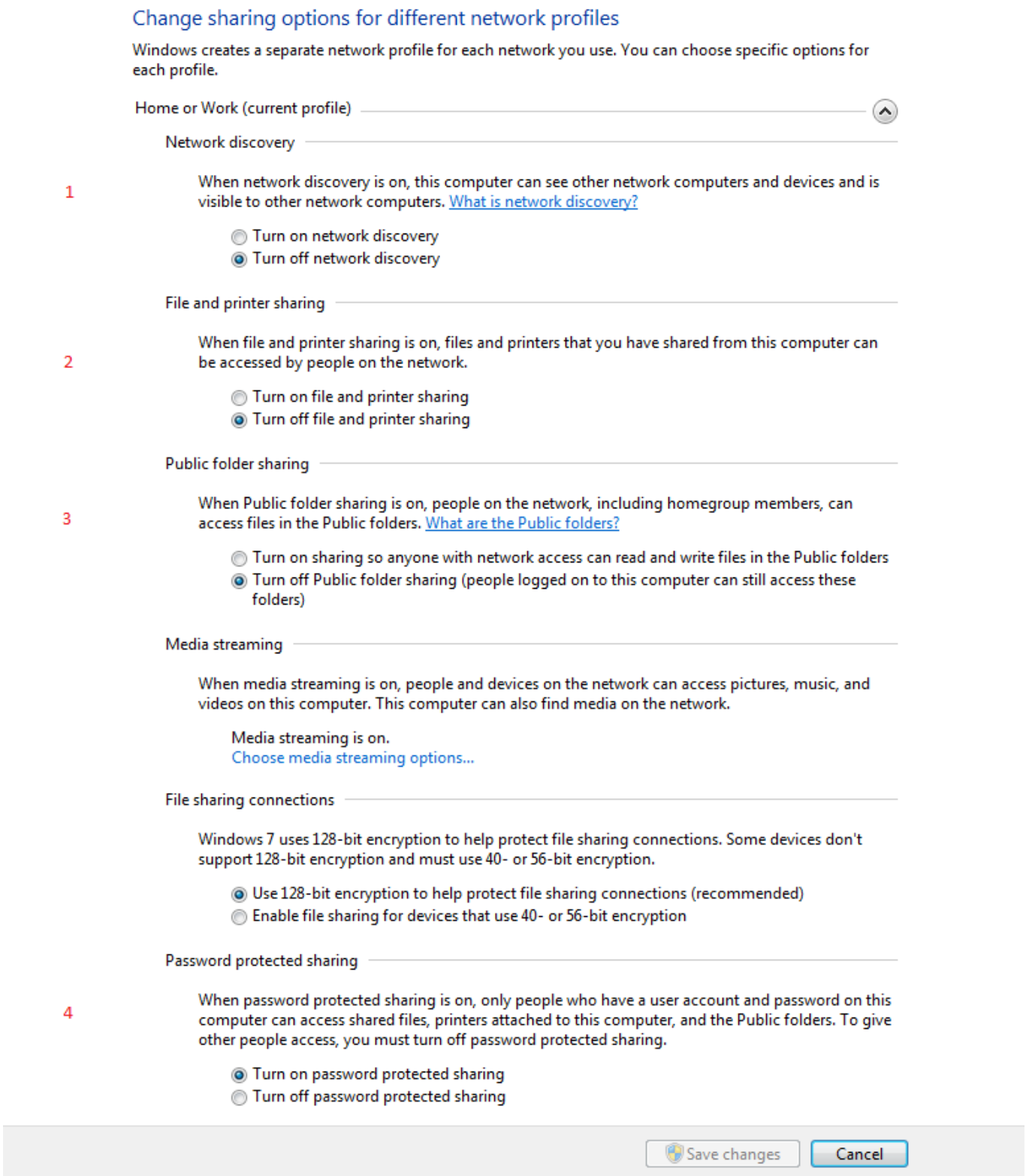
Tietoturvayhtiö McAfee:n julkaisema SiteAdvisor –sovellus, joka toimii selaimeen asennettavana lisäosana, näyttää hakukoneen hakutulosten sivujen turvallisuuden linkin vieressä. Jos käyttäjä päätyy haitalliselle sivulle nettisurffailun myötä, SiteAdvisor varmistaa käyttäjältä, haluaako tämä varmasti mennä kyseiselle sivulle (SiteAdvisor 2013). SiteAdvisor ei ole täysin tarkka, sillä välillä SiteAdvisor saattaa ilmoittaa turvallisen sivun olevan epäluotettava, mutta useimmiten kokematon käyttäjä välttyy ikävämmiltä haittaohjelmilta SiteAdvisorin kaltaisten lisäosien ansiosta.

Ponnahdusikkuna, eli pop-up –mainokset, saattavat häiritä nettisurffailua ja huonolla onnella mainoksen klikkaaminen saattaa johdattaa käyttäjän haitalliselle sivulle. Näiltä mainoksilta voi välttyä käyttämällä selaimen AdBlock –lisäosaa, joka estää ponnahdusikkunoiden avautumisen.

Tiedostojen ja verkkoresurssien jakaminen

Monet käyttöjärjestelmät tukevat tiedostojen ja verkkoresurssien jakamista. Pienissä kotiverkoissa tämä voi olla kätevä ratkaisu saman kansion tai tulostimen jakamiseen useammalle koneelle, mutta huolimattomasti säädetyt jako-ominaisuudet saattavat vahingossa tehdä verkosta ja jaetuista tiedostoista näkyviä kaikille saman verkon, esimerkiksi taloyhtiön jaetun verkon, koneille. Tästä syystä tiedostojen ja resurssien jakamiset olisi hyvä kytkeä kokonaan pois päältä (Kuva 11), jos taloudessa on vain yksi kone tai jos käyttäjällä ei ole aikomusta jakaa tiedostoja tai resursseja toisen koneen kanssa.

Jakamisominaisuudet säädetään eri käyttöjärjestelmissä eri tavoin. Internetistä löytyy ohjeet kunkin käyttöjärjestelmän jako-ominaisuuksien säätämiseen.



Kuva 11. Windows 7 jako-ominaisuudet. Huomaa numeroidut kohdat.

10.2 Vahinkojen minimointi

Vaikka käyttäjä olisi miten varovainen hyvänsä, koneelle voi kaikesta huolimatta ilmaantua haittaohjelmia. Varovainen käyttäjä voi kuitenkin välttyä vakavimmilta haittaohjelmilta. Vahinkoja voi myös syntyä laiterikon yhteydessä, joten vastoinkäymisiin kannattaa varautua hyvissä ajoin.

Tiedostojen menetyksestä toipuminen

Tiedostojen tuhoutuminen tai korruptoituminen on tavanomainen esimerkki vahingosta, joka voi tapahtua monesta syystä. Tietojen häviäminen voi johtua esimerkiksi sellaisen haittaohjelman poistamisesta, joka edellyttää käyttöjärjestelmän uudelleenasennusta, mutta tiedostojen häviäminen voi johtua myös kiintolevyn rikkoutumisesta. Laitevialle peruskäyttäjä ei voi tehdä mitään, joten tärkeiden tietojen varmuuskopiointi ulkoiselle tallennusmedialle, kuten USB-muistitikulle, ja varmuuskopioiden päivittäminen säästävät aikaa ja vaivaa. Vahinkojen syntymistä ei voi aina ennakoida, joten tärkeät tiedostot kannattaa varmuuskopioida usein, tärkeydestä riippuen joko kerran kuukaudessa tai viikoittain.

Tietojen kryptaus

Jos koneella on erityisen arvokasta tietoa, käyttäjä voi harkita tiedostojen salakirjoitusta. Salaamiseen on olemassa monia eri tapoja ja eri sovelluksia. Liitteessä 1 on esitetty esimerkki kryptauksesta käyttäen ilmaisohjelmaa AxCrypt.

10.3 Tietovuotojen ennaltaehkäisy

Tietomurron seurauksena voi tapahtua tietovuoto, mutta tietovuoto voi tapahtua myös käyttäjän omasta virheestä tai huolimattomuudesta. Julkiselle paikalle unohtunut muistitikku, arkaluonteista tietoa sisältävä dokumentti, keskenjäänyt

uloskirjautuminen sekä arkaluontoisten dokumenttien huolimaton käsittely julkisilla paikoilla ovat tavanomaisia esimerkkejä henkilön itse aiheuttamasta tietovuodosta. Tästä syystä on tärkeää, että yritykset antavat selkeät ohjeistukset ja määräykset työhön liittyvien tietojen käsittelyn suhteen. Sama koskee myös yksittäisiä peruskäyttäjiä. Etenkin, jos kyseiset henkilöt käyttävät julkisia koneita asioidessaan verkkopalveluissa.

Tiedostojen asianmukainen säilytys

Tärkeää tai arkaluonteista tietoa sisältävä tiedosto, sekä liitetiedostoja sisältävät sähköpostit, tulisi poistaa heti sen jälkeen, kun tiedostoa ei enää tarvita. Ennen poistamista on kuitenkin suositeltavaa varmistaa, että tiedostosta on tehty varmuuskopio hyvin suojattuun kohteeseen, joko palvelimelle tai lukkojen takana säilytettävälle ulkoiselle massamuistilaitteelle, mahdollista myöhempää käyttöä varten. Mitä vähemmän arkaluonteisia tiedostoja henkilön tietokoneelta tai verkkopalvelusta löytyy, sen pienempi vaikutus yksittäishenkilön virheestä syntyneellä tietovuodolla on.

Tiedostojen ylikirjoittaminen

Arkaluonteisia tiedostoja poistaessa on syytä harkita tiedostojen ylikirjoittamista. Tavallisin keinoin poistettuja tiedostoja voidaan jälkeenpäin palauttaa tietokoneen kiintolevyltä siltä varalta, että käyttäjä vahingossa poistaa tarvitsemansa tiedoston, mutta ylikirjoittamisella tiedostoja voidaan poistaa pysyvästi koneen kiintolevyltä. Tiedostojen ylikirjoitus estää tehokkaasti tahattomat tietovuodot. Tästä on esimerkkinä tilanne, jossa vanhasta koneesta siirretään kiintolevy, jolla on säilytetty arkaluonteisia tiedostoja, uuteen koneeseen. Mitä useamman kerran sama kohta kiintolevystä ylikirjoitetaan, sitä pienemmällä todennäköisyydellä poistettu tiedosto voidaan palauttaa. Kun sama osa kiintolevystä on ylikirjoitettu riittävän useasti, poistettua tiedostoa on käytännössä mahdotonta palauttaa.

Tiedostojen ylikirjoittamiseen on olemassa useita ohjelmia. Liitteen 2 esimerkissä on käytetty peruskäyttäjälle soveltuvaa ilmaisohjelmaa Eraser.

11 YHTEENVETO

Opinnäytetyön päätavoitteena oli kartoittaa miksi ja miten tietomurtoja tapahtuu sekä selvittää lukijalle tietoturvan huolehtimisen tärkeyttä, oli hän sitten peruskäyttäjä tai kokeneempi käyttäjä. Työn sisältö on teoriapainotteista, koska haittaohjelmien ja rikollisten torjuminen edellyttää, että käyttäjä tietää teoriassa kyseisten sovellusten ja henkilöiden käyttämät metodit sekä tavoitteet.

Työn yhtenä ongelmana voidaan pitää tietotekniikan, haittaohjelmien ja murtomenetelmien nopeaa kehittymistä, minkä seurauksena työn asiasisältö on jo muutaman vuoden päästä vanhentunutta tietoa.

Työn teoriaosuudessa selvitettiin hakkereiden eroavaisuuksia, mitä rikolliset tekevät varastamillaan tiedoilla ja mitä seurauksia tietomurroilla on. Työssä on lueteltu esimerkkejä rikollisten aiheuttamista vahingoista, jotka luultavasti olisivat jääneet toteutumatta tai olisivat tehneet huomattavasti vähemmän vahinkoa, jos kohteena olleet henkilöt ja yritykset eivät olisi laiminlyöneet tietoturvastaan huolehtimista. Opinnäytetyön kohdeyleisönä ovat yksityishenkilöt, minkä vuoksi sisältö on pyritty laatimaan helposti luettavaksi, mutta kuitenkin niin perusteelliseksi, että myös aiheeseen perehtyneet oppivat työstä uusia asioita.

Työn lopputuloksena syntyi dokumentaatio tietomurtojen historiasta, tietoturvan yleisistä kompastuskivistä sekä ohjeita tietoturvan ylläpitoon.

LÄHTEET

The 414s 2012. Wikipedia. Viitattu 25.9.2012 http://en.wikipedia.org/wiki/The_414s.

ABC News 2013. Self-proclaimed LulzSec leader arrested in NSW. Viitattu 3.10.2013 http://www.abc.net.au/news/2013-04-24/lulz-security-hacking-leader-arrested-in-nsw/4648134.

Albert Gonzalez 2013. Wikipedia. Viitattu 8.5.2013 http://en.wikipedia.org/wiki/Albert_Gonzalez.

Andress, J. 2011. The Basics of Information Security : Understanding the Fundamentals of InfoSec in Theory and Practice. Massachusetts: Syngress Media Incorporated.

BBC News 2013. Hackers warn NHS over security. Viitattu 3.10.2013 http://www.bbc.co.uk/news/technology-13712377.

Beast Trojan horse 2012. Wikipedia. Viitattu 27.11.2012 http://en.wikipedia.org/wiki/Beast_(Trojan_horse).

Bennett-Smith, M. 2012. Anonymous Declares War On Syrian Government Websites In Retaliation For Internet Blackout. Viitattu 31.1.2013 http://www.huffingtonpost.com/2012/11/30/anonymous-declares-war-syrian-government-websites_n_2218447.html.

Botti 2013. Wikipedia. Viitattu 16.9.2013 http://fi.wikipedia.org/wiki/Botti.

Bright, P. 2011. Titanic Takeover Tuesday: LulzSec's busy day of hacking escapades. Arstechnica. Viitattu 24.10.2013 http://arstechnica.com/tech-policy/2011/06/titanic-takeover-tuesday-lulzsecs-busy-day-of-hacking-escapades/.

Bumiller, E. 2010. Video Shows U.S. Killing of Reuters Employees. The New York Times. Viitattu 24.10.2013 http://www.nytimes.com/2010/04/06/world/middleeast/06baghdad.html?_r=0.

Cantwell, O. 2008. Hemliga dokument fanns på bibliotek. Aftonbladet. Viitattu 24.10.2013 http://www.aftonbladet.se/nyheter/article1563893.ab

Coleman, G. 2011. Anonymous: From the Lulz to Collective Action. The New Everyday. Viitattu 2.10.2013 http://mediacommons.futureofthebook.org/tne/pieces/anonymous-lulz-collective-action.

Computer Security Review 2012. FAQ -> Spyware -> Is Adware dangerous? Viitattu 23.10.2012 http://www.computer-security-review.org/faqs/spyware/is-adware-dangerous.html.

Edwards, C. & Riley, M. 2011. Sony Data Breach Exposes Users to Years of Identity-Theft Risk. Bloomberg. Viitattu 24.10.2013 http://www.bloomberg.com/news/2011-05-03/sony-breach-exposes-users-to-identity-theft-as-credit-card-threat-recedes.html.

Ethicalhack3r 2013. Old School Hacking, NetBus. Viitattu 23.1.2013 http://www.ethicalhack3r.co.uk/old-school-hacking/.

Faustus, R. 2010. Online Fraud Cases - A Look Into One of the Largest Online Fraud Cases in U.S. History. Bright Hub. Viitattu 24.10.2013 http://www.brighthub.com/internet/security-privacy/articles/71634.aspx.

FindingDulcinea 2013. On This Day: Robert Tappan Morris Becomes First Hacker Prosecuted for Spreading Virus. Viitattu 3.10.2013 http://www.findingdulcinea.com/news/on-this-day/July-August-08/On-this-Day--Robert-Morris-Becomes-First-Hacker-Prosecuted-For-Spreading-Virus.html.

GR INFOLAB 2013. Viitattu 10.1.2013 http://www.infolab-gr.com/2012/07/o-que-e-rootkit.html.

Greene, T. 2003.Chapter One: Kevin Mitnick's story. The Register 2013. Viitattu 23.8.2013 http://www.theregister.co.uk/2003/01/13/chapter_one_kevin_mitnicks_story/.

Goldman, D. 2013. Shodan: The scariest search engine on the Internet. CNNMoney. Viitattu 24.10.2013 http://money.cnn.com/2013/04/08/technology/security/shodan/index.html.

Gots, J. 2011.Hacker for the Hell of It: The Adventures of Kevin Mitnick. Viitattu 24.10.2013 http://bigthink.com/think-tank/hacker-for-the-hell-of-it-the-adventures-of-kevin-mitnick.

Halliday, J. & Arthur, C. 2010. WikiLeaks: Anonymous hierarchy emerges. The Guardian. Viitattu 24.10.2013 http://www.theguardian.com/media/2010/dec/16/wikileaks-anonymous-hierarchy-emerges.

Hintikka, K. 2013. Kansalaisyhteiskunnan tutkimusportaali - Haktivismi. Jyväskylän yliopisto. Viitattu 21.10.2013 http://kans.jyu.fi/sanasto/sanat-kansio/haktivismi.

Holland, S. & Mikkelsen, R. 2009. UPDATE 2-US concerned power grid vulnerable to cyber-attack. Reuters. Viitattu 24.10.2013 http://in.reuters.com/article/2009/04/08/cyberattack-usa-idINN0853911920090408.

Information Systems Security 2013. Stealing Information and Exploitation: Form Grabbing. Viitattu 5.2.2013 http://www.infosectoday.com/Articles/Form_Grabbing/Form_Grabbing.htm.

The Jargon File 2013a. Cracker. Viitattu 2.10.2013 http://www.catb.org/jargon/html/C/cracker.html.

The Jargon File 2013b. Backdoor. Viitattu 14.10.2013 http://catb.org/jargon/html/B/back-door.html.

Kahney, L. 2003. Live on the Web: Kevin Mitnick. Wired. Viitattu 2.10.2013 http://www.wired.com/techbiz/it/news/2003/01/57338.

Kirk, J. 2010. Zeus malware used pilfered digital certificate. IT News. Viitattu 24.10.2013 http://www.itnews.com/desktop-security/20953/zeus-malware-used-pilfered-digital-certificate.

Krebs, B. 2010. ‘Stuxnet’ Worm Far More Sophisticated Than Previously Thought. Krebs on Security. Viitattu 16.9.2013 http://krebsonsecurity.com/2010/09/stuxnet-worm-far-more-sophisticated-than-previously-thought/.

Laurio, J-M. 2009. Historian vanhin tietomurto löytyi. Tietoviikko. Viitattu 24.10.2013 http://www.tietoviikko.fi/kaikki_uutiset/historian+vanhin+tietomurto+loytyi/a294091?service=mobile&page=2.

Leyden, J. 2013. Who is the mystery sixth member of LulzSec? The Register. Viitattu 24.10.2013
http://www.theregister.co.uk/2013/05/17/lulzsec_analysis/.

Li, H. 2011. Who is LulzSec, Hacker of PBS? Are they hacking Sony again? Viitattu 3.10.2013 http://www.ibtimes.com/who-lulzsec-hacker-pbs-are-they-hacking-sony-again-287315.

Los Alamos National Laboratory 2012. Wikipedia. Viitattu 25.9.2012 http://en.wikipedia.org/wiki/Los_Alamos_National_Laboratory.

McDonough, M. 2013. Guide to Phishing: Internet Scams and Emails. BrightHub. Viitattu 21.10.2013
http://www.brighthub.com/internet/security-privacy/articles/63357.aspx.

McMillan, G. 2013. Sony fined almost 400,000 for 2011 Playstation security breach. Digital Trends. Viitattu 24.10.2013 http://www.digitaltrends.com/gaming/sony-fined-almost-400000-for-2011-playstation-security-breach/.

Microsoft 2013. Conficker Worm. Viitattu 21.10.2013 http://www.microsoft.com/security/pc-security/conficker.aspx.

Mitnick Security Consulting 2013. Viitattu 2.10.2013 http://mitnicksecurity.com/.

Nakashima, E. 2011. CIA Web site hacked; group LulzSec takes credit. The Washington Post. Viitattu 24.10.2013 http://www.washingtonpost.com/national/national-security/cia-web-site-hacked/2011/06/15/AGGNphWH_story.html.

Olson, P. 2013. Despite All The Fuss, Trademarked Anonymous Logo 'Might Not Be Valid'. Forbes. Viitattu 21.10.2013. http://www.forbes.com/sites/parmyolson/2012/08/02/despite-all-the-fuss-trademarked-anonymous-logo-might-not-be-valid/.

Protalinski, E. 2012. Anonymous attacks over 650 Israeli sites. The Next Web. Viitattu 24.10.2013
http://thenextweb.com/insider/2012/11/17/anonymous-takes-down-countless-israeli-sites-wipes-databases-leaks-emails-addresses-and-passwords/.

Rajnish, K. 2012. Top 10 Most Dangerous Computer Viruses of the Decade Updated 2012. Tech Twisted. Viitattu 24.10.2013 http://techtwisted.com/top-10-dangerous-computer-viruses-decade-updated-2012/.

Rouse, M. 2005. What is war driving (access point mapping)? SearchMobileComputing. Viitattu 24.10.2013
http://searchmobilecomputing.techtarget.com/definition/war-driving.

Schectman, J. 2012. Skype Knew of Security Flaw Since November 2010, Researchers say. The Wall Street Journal. Viitattu 24.10.2013 http://blogs.wsj.com/cio/2012/05/01/skype-knew-of-security-flaw-since-november-2010-researchers-say/.

SHODAN 2013. SHODAN - computer Search Engine -> Learn More. Viitattu 24.9.2013 http://www.shodanhq.com/help.

SiteAdvisor 2013. McAfee SiteAdvisor -> Learn More. Viitattu 24.9.2013 http://www.siteadvisor.com/howitworks/index.html.

Sutton, J. 2007. Guantanamo operating manual posted on Internet. Reuters. Viitattu 24.10.2013 http://www.reuters.com/article/2007/11/14/us-guantanamo-manual-idUSN1424207020071114?pageNumber=1.

Vanhala, L 2012. Tietomurrot: Mitä varastetuilla tiedoilla voi tehdä? Suomen kuvalehti. Viitattu 9.11.2012 http://suomenkuvalehti.fi/jutut/kotimaa/tietomurrot-mita-varastetuilla-tiedoilla-voi-tehda.

Symantec 2012. What are malware, viruses, Spyware, and cookies, and what differentiates them? Viitattu 23.10.2012 http://www.symantec.com/connect/articles/what-are-malware-viruses-spyware-and-cookies-and-what-differentiates-them.

Symantec 2013. SpySheriff -> Technical Details. Viitattu 21.10.2013 http://www.symantec.com/security_response/writeup.jsp?docid=2005-122910-4625-99.

The TEXTFILES.COM 2012. August 1983. Viitattu 25.9.2012 http://timeline.textfiles.com/1983/.

TMRC 2013. Hackers. Viitattu 2.10.2013 http://tmrc.mit.edu/hackers-ref.html.

Waiters, R. 2011. V for Vendetta masks: Who's behind them? BBC News. Viitattu 24.10.2013 http://www.bbc.co.uk/news/magazine-15359735.

The Washington Post 2013. Timeline: The U.S. Government and Cybersecurity. Viitattu 3.10.2013 http://www.washingtonpost.com/wp-dyn/articles/A50606-2002Jun26.html.

Williamson, E. 2007. Freedom of Information, the Wiki Way. The Washington Post. Viitattu 24.10.2013 http://www.washingtonpost.com/wp-dyn/content/article/2007/01/14/AR2007011400760.html.

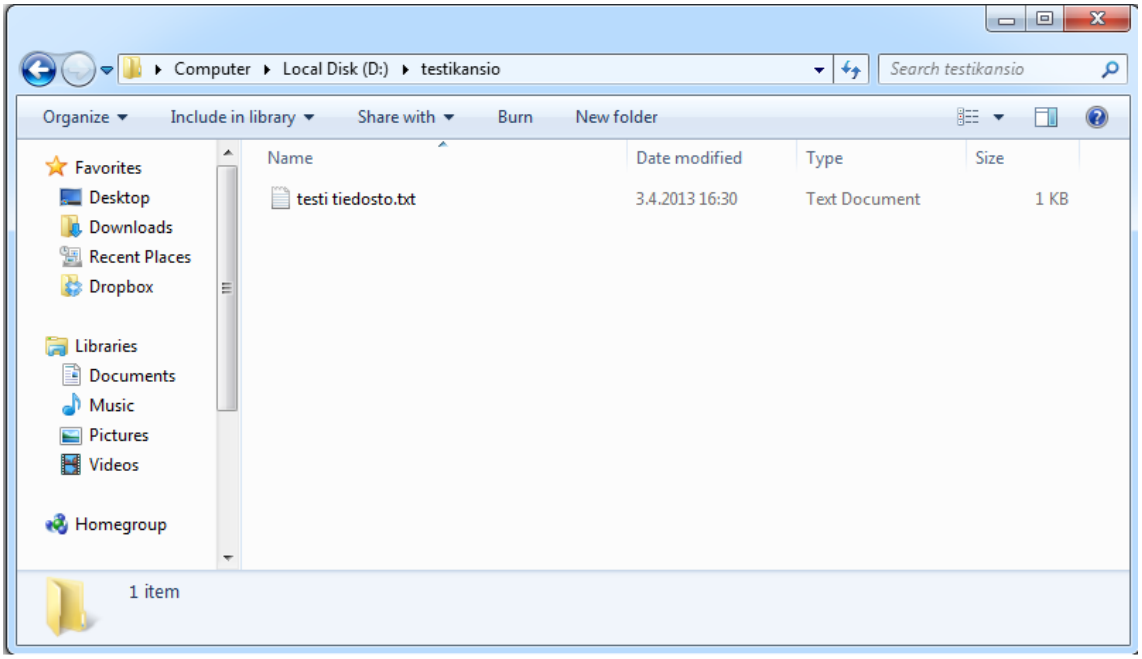
Winter, J. 2012. EXCLUSIVE: Infamous international hacking group LulzSec brought down by own leader. Viitattu 3.10.2013 http://www.foxnews.com/tech/2012/03/06/hacking-group-lulzsec-swept-up-by-law-enforcement/.

ZSecurity 2013. Rootkit: Definition, Prevention and Removal. Viitattu 3.10.2013 http://www.zsecurity.com/articles-rootkits.php.

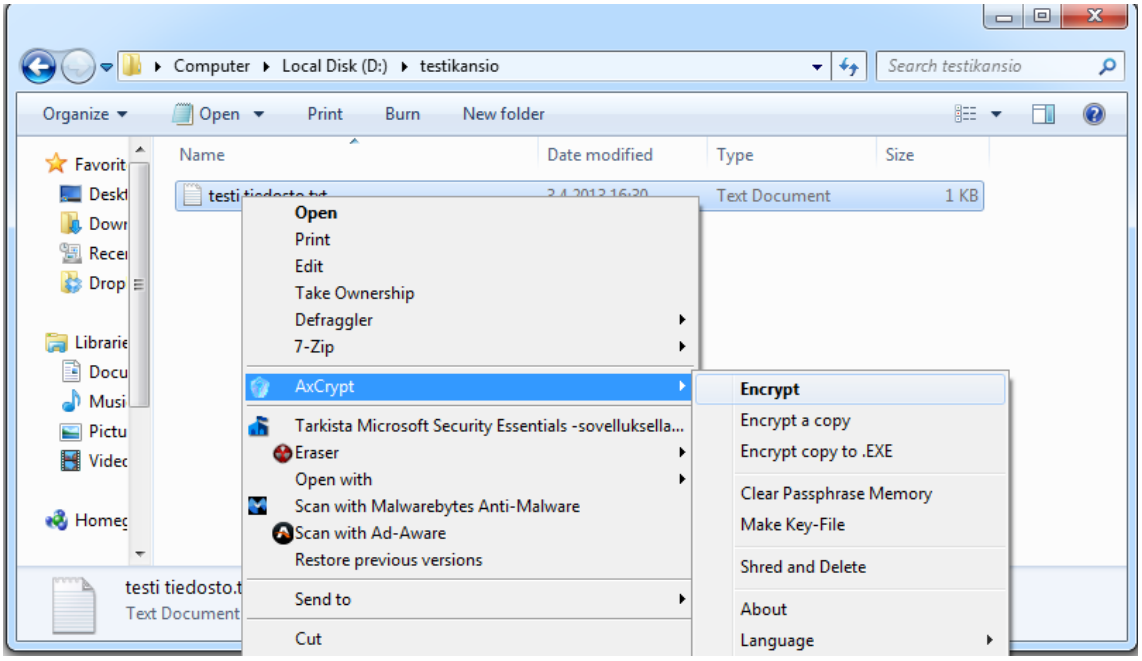
Åström-Kupsanen, M 2012. Identiteettivarkaus sekoittaa elämän. Kuningaskuluttaja. Viitattu 12.11.2012 http://kuningaskuluttaja.yle.fi/node/3011.

Tiedoston kryptaus

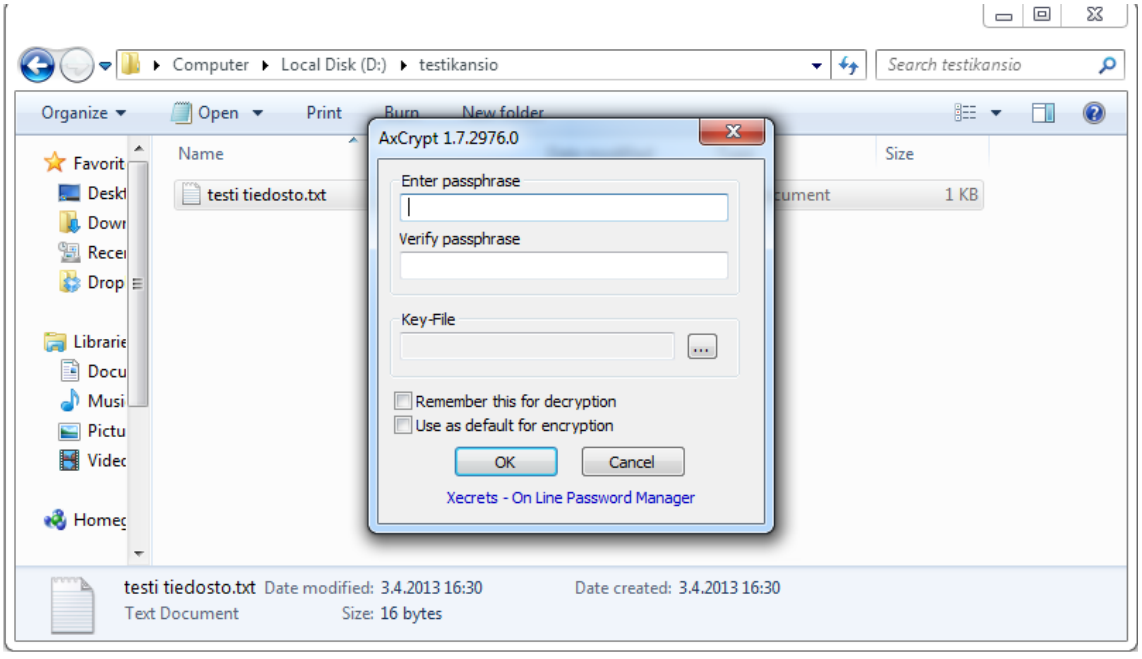
”testi tiedosto.txt” sijaitsee kansiossa D:\testikansio (Kuva 12). ”testi tiedosto.txt” halutaan kryptata mahdollisen tietomurron tai tietovuodon vahinkojen minimoimiseksi.



Kuva 12. Tilanne ennen kryptausta.



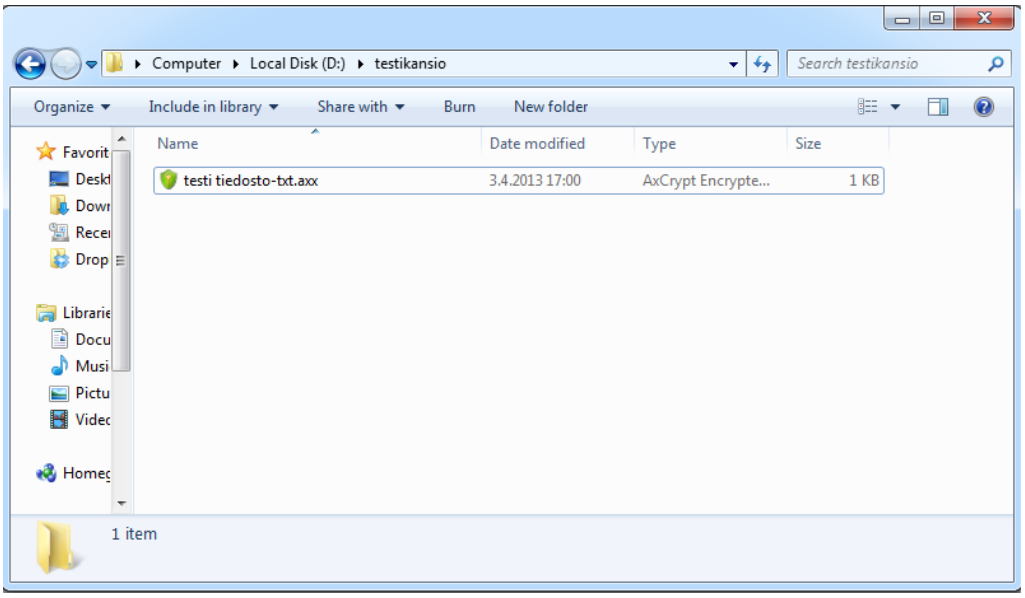
Kuva 13. AxCrypt, valitaan **Encrypt.**



Kuva 14. Passphrase –salaus.

”testi tiedosto.txt” –tiedosto suojataan käyttämällä AxCrypt –sovellusta (Kuva 13) ja käyttämällä ”passphrase” menetelmää (Kuva 14). ”Passphrase” toimii kuten salasanasuojaus, käyttäjä saa avattua tiedoston, kun käyttäjä syöttää oikean salasanan. Esimerkissä käytettyä salasanaa ”Testi” ei suositella käytettä-

väksi tiedostojen kryptauksessa. Onnistuneen kryptauksen seurauksena tiedostopääte muuttuu muotoon .**axx** (Kuva 15).

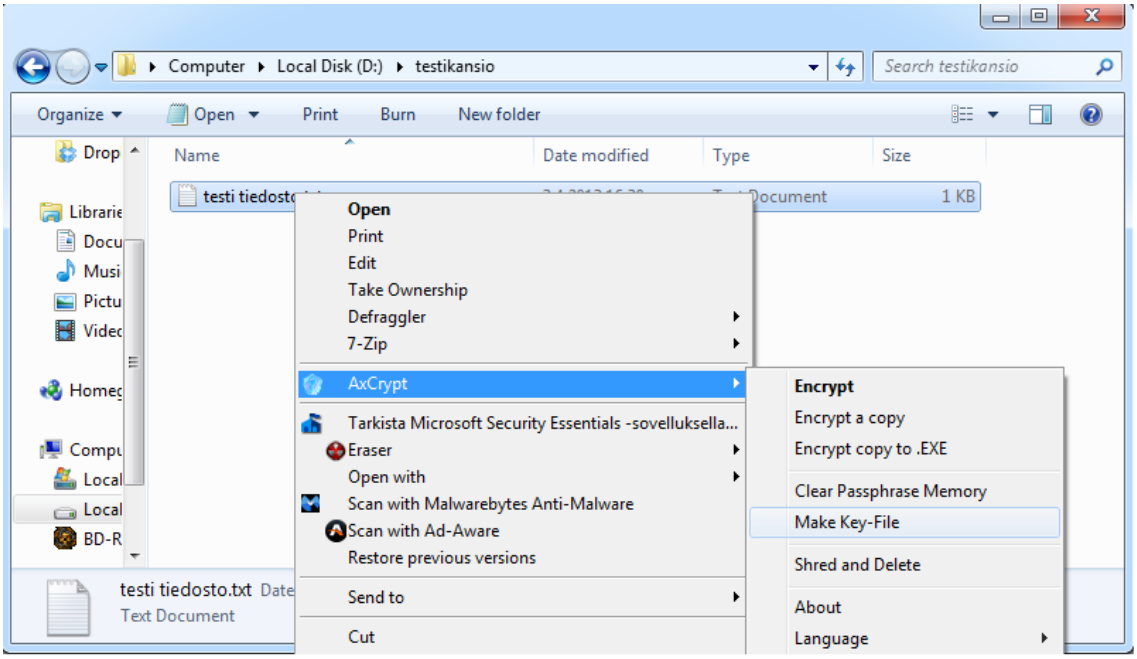


Kuva 15. testi tiedosto.txt kryptauksen jälkeen. Huomaa tiedostopääte .axx.

”Passphrase” –salauksella kryptattu tiedosto puretaan klikkaamalla hiiren oikealla painikkeella **testi tiedosto.axx** > **Decrypt** (Kuva 13, **Encrypt** -tekstin tilalla **Decrypt**).

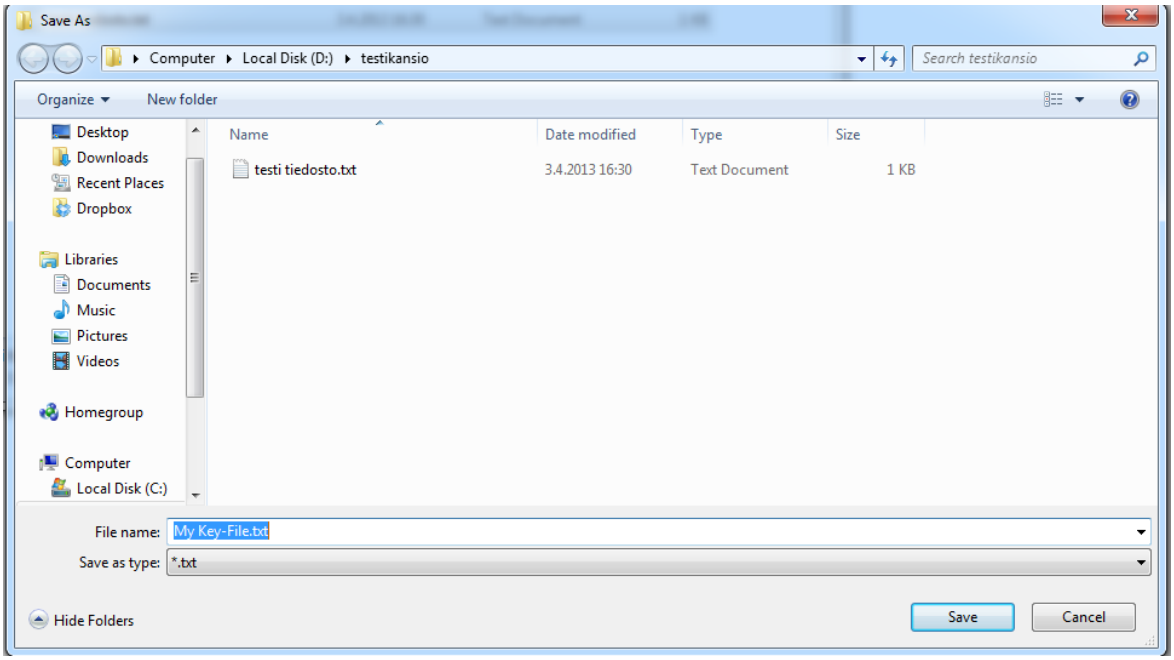
Syötä ”Enter passphrase” –tekstikenttään salasana, jolla tiedosto on salattu (esimerkissä käytetty salasanaa ”Testi”) ja paina OK. Tämän jälkeen ”testi tiedosto.txt” näkyy kansiossa .txt -muodossa kuten alkutilanteessa (Kuva 12). Jos käyttäjä ei halua purkaa salausta, mutta haluaa kuitenkin tarkastella tiedoston sisältöä, valitse **AxCrypt > Decrypt** -komennon sijaan **Open** (Kuva 13, valikon ylin komento).

Kryptauksen voi myös tehdä salausavainta käyttäen. Salauksen tekevä henkilö luo salausavaimen ja toimittaa kopion salausavaimesta tiedoston vastaanottajille. Salausavain generoidaan satunnaisesti kryptauksen yhteydessä, joten sitä on huomattavasti vaikeampi murtaa kuin selkokielistä salasanaa ja sitä on käytännössä mahdotonta arvata. Salausavaimella suojattu tiedosto tehdään AxCrypt –sovelluksella noudattamalla samoja ohjeita kuin edellä, mutta **Encrypt** -komennon sijaan valitaan **Make Key-File** (Kuva 16).



Kuva 16. AxCrypt, valitaan Make Key-File.

AxCrypt kehottaa käyttäjää tallentamaan avaimen ainoastaan ulkoiselle massamuistilaitteelle (esimerkiksi USB-muistitikku, verkkolevy tai Dropbox). On kuitenkin muistettava, että avaimella suojattuja tiedostoja ei saa auki, jos avain katoaa!

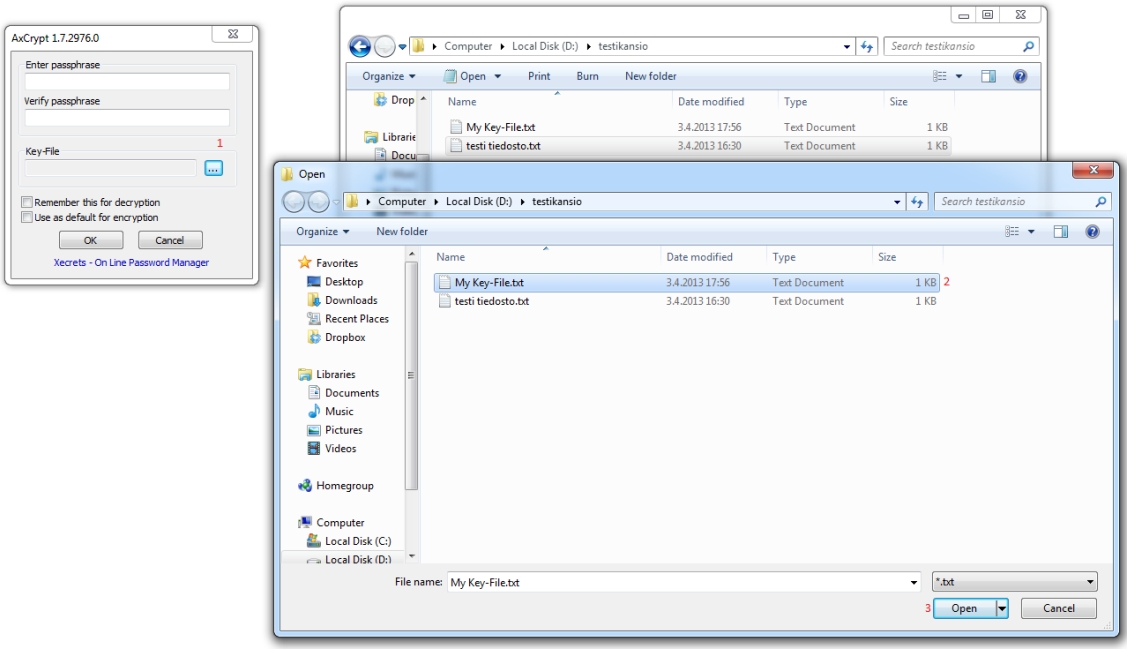


Kuva 17. Salausavaimen tallennus.

AxCrypt ehdottaa avaimen oletusnimeksi ”My Key-File.txt. Salausavain tallentuu selkokielisenä tekstitiedostona, jota käytetään myöhemmin salauksen purkamiseen. Esimerkissä salausavain on tallennettu samaan kansioon kuin salattava tiedosto (Kuva 17), mutta oikeaa salausta tehdessä salausavain tulisi ehdottomasti tallentaa suojaisampaan paikkaan. Tähän tarkoitukseen sopii esimerkiksi lukkojen takana säilytettävä muistitikku.

Avaimen tallentamisen jälkeen kansiossa D:\testikansio on kaksi tiedostoa, ”testi tiedosto.txt” sekä ”My Key-File.txt”. Äsken luotua avaintiedostoa käytetään tiedoston ”testi tiedosto.txt” kryptaamiseen.

Valitse hiiren oikealla painikkeella **testi tiedosto.txt** > **Encrypt** (Kuva 16).



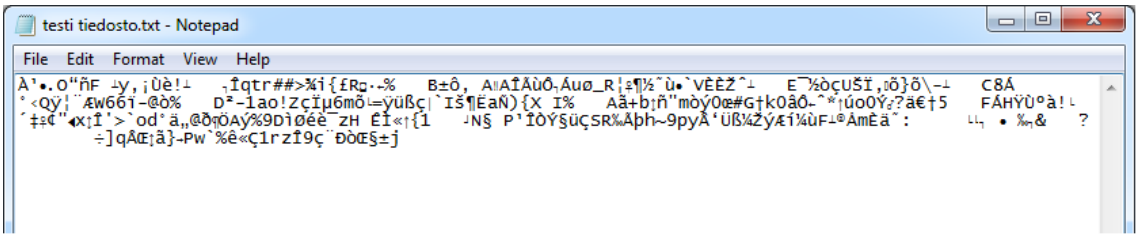
Kuva 18. Salausavaimen linkittäminen salattavaan tiedostoon.

Paina ”**Key File**” –tekstikentän viereistä ”…”–painiketta (Kuva 18, kohta 1), hae salauksessa käytetty avain (Kuva 18, kohta 2) ja paina lopuksi ”Open” (Kuva 18, kohta 3). Tiedosto on nyt salattu salausavaimella ja tiedostopääte on muuttunut .**axx** -päätteiseksi kuten kuvassa 15. Jos käyttäjä aikoo lähettää salatun tiedoston eteenpäin, hänen tulee toimittaa salausavain vastaanottajalle. Salausavaimella suojattu tiedosto puretaan seuraamalla kuvan 18. ohjeistusta sillä

erotuksella, että **Encrypt** –käskyn sijaan käytetään **Decrypt** –käskyä (**Decrypt** –käsky ilmestyy AxCryptin valikkoon automaattisesti **Encrypt** -käskyn tilalle kun käsitellään .**axx** -päätteistä tiedostoa).

Kryptauksen hyödyn näkee parhaiten, kun muuttaa käsin **testi tiedosto-txt.axx** tiedoston nimen muotoon **testi tiedosto.txt** ja avaa uudelleennimetyn tiedoston (Kuva 19 ja 20).

Kuva 19. ”testi tiedosto.txt” ilman kryptausta.

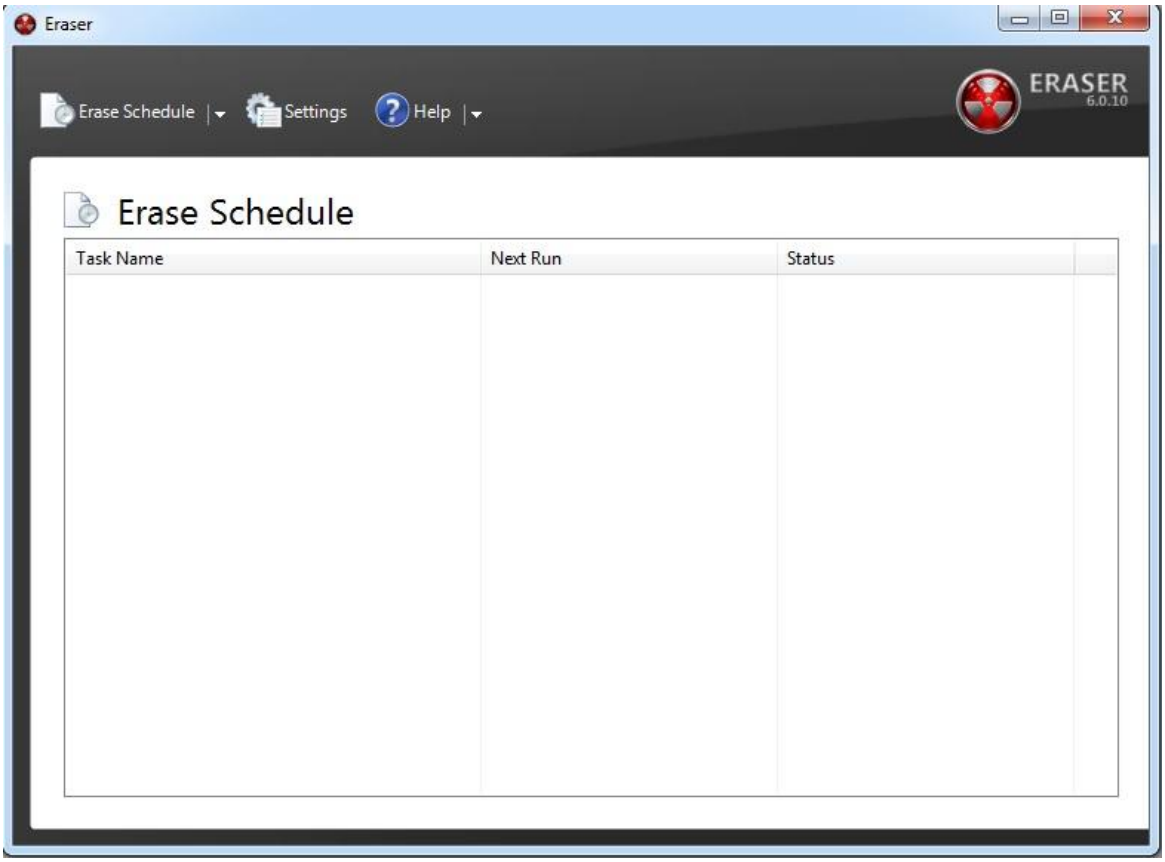


Kuva 20. ”testi tiedosto.txt” kryptattuna.

.

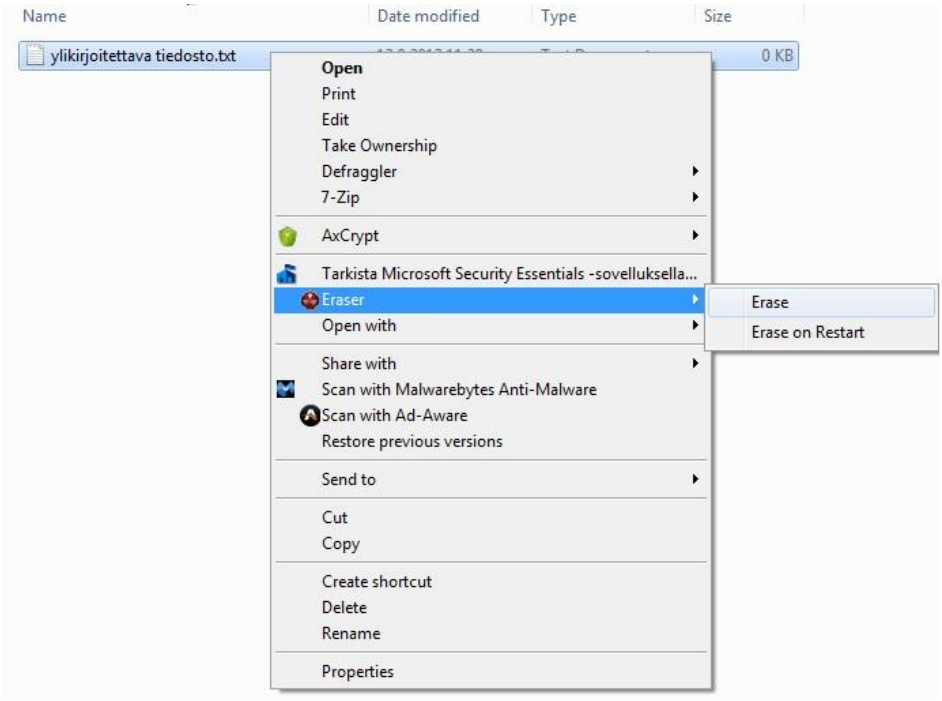
Tiedostojen ylikirjoittaminen

Tiedostojen ylikirjoittamisella varmistetaan, että poistettua tiedostoa ei voida palauttaa poistamisen jälkeen. Tästä on erityisesti hyötyä käsitellessä sellaisia tiedostoja, jotka sisältävät arkaluonteista tietoa tai ne tarvitsee hävittää, kun niitä ei enää tarvita.



Kuva 21. Eraser –sovellus.

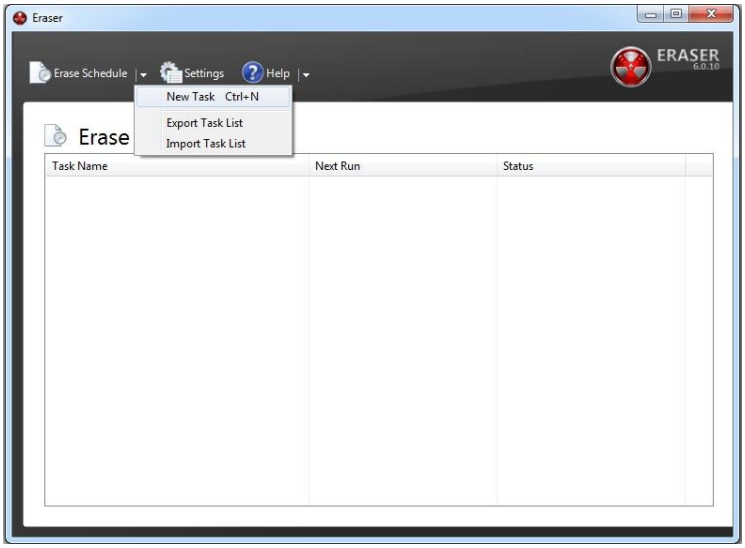
Eraser –sovellusta voidaan käyttää joko manuaalisesti tiedostojen yksittäiseen poistamiseen (Kuva 22) tai automatisoida sovellus ylikirjoittamaan esimerkiksi Roskakoriin siirretyt tiedostot säännöllisin väliajoin. AxCrypt –sovelluksen tavoin Eraser –sovellusta käytetään hiiren kakkospainikkeella avautuvan valikon kautta. Yksittäistä tiedostoa poistaessa riittää, että käyttäjä valitsee ylikirjoitettavan tiedoston (esimerkissä ”ylikirjoitettava tiedosto.txt”) ja valitsee **Eraser > Erase** –komennon (Kuva 22).



Kuva 22. Eraser, manuaalinen ylikirjoitus.

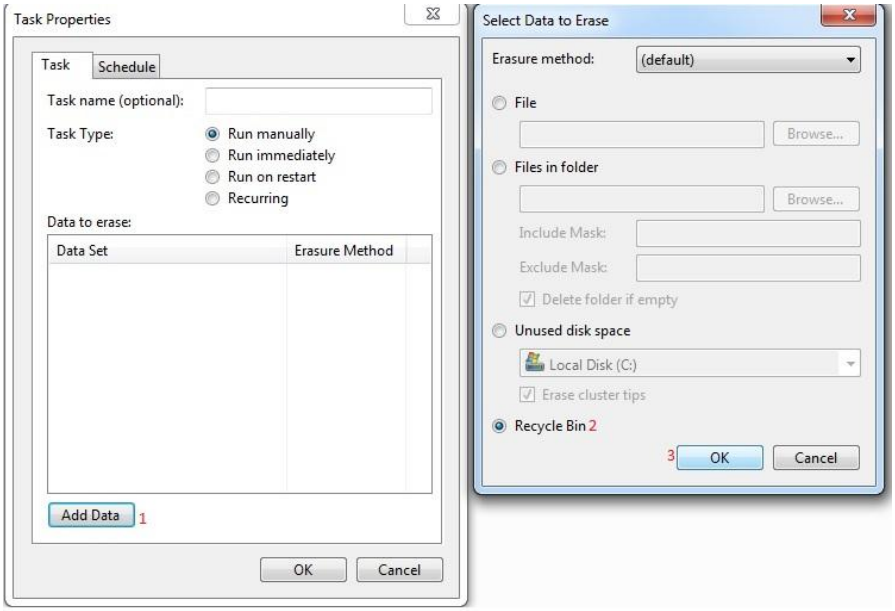
Automatisoidun ylikirjoituksen ajastaminen tehdään seuraavasti:

Paina **Erase Schedule** otsikon viereistä nuolta, valitse **New Task** (Kuva 23).



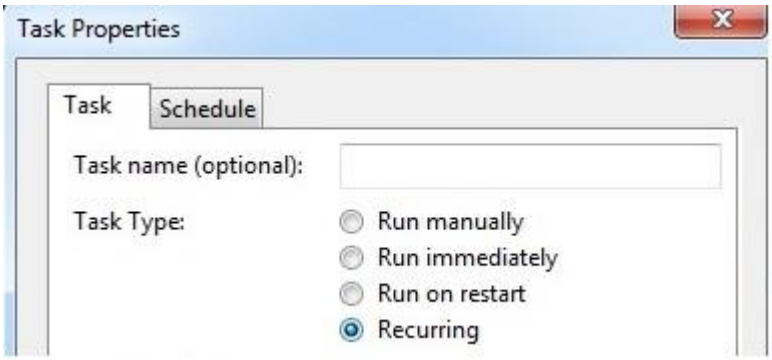
Kuva 23. Eraser, New Task.

Valitse **Add Data** -> **Recycle Bin** ja klikkaa Ok (kuva 24).



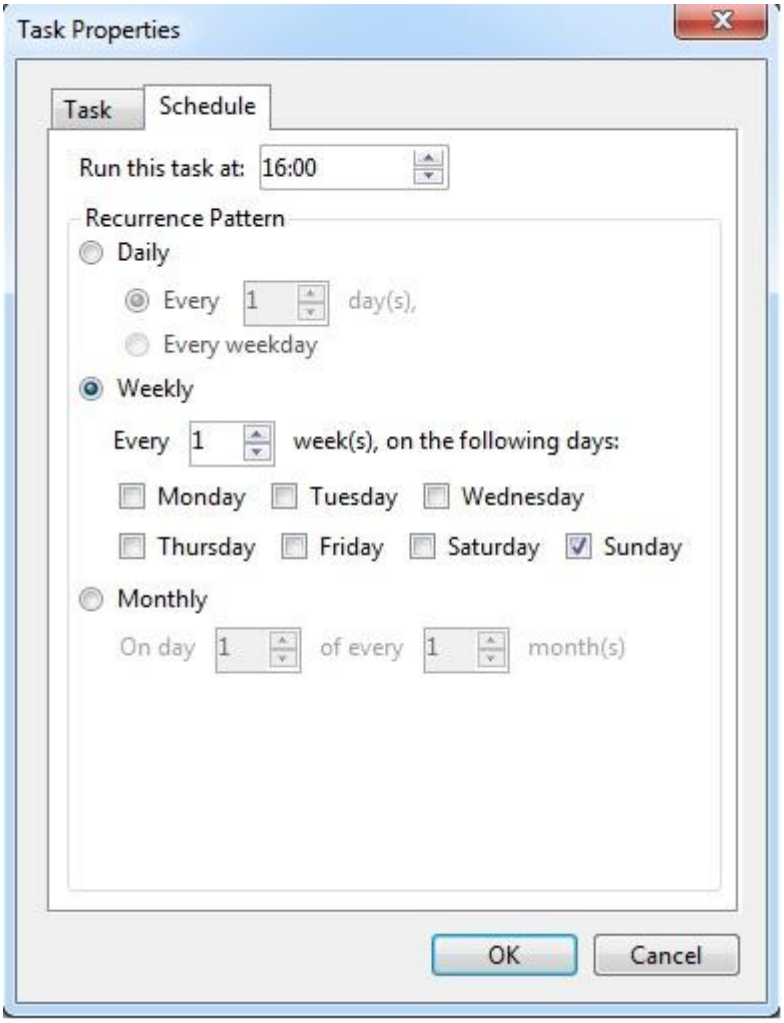
Kuva 24. Eraser, työn lisääminen.

Valitse **Task Type: Recurring** (Kuva 25).



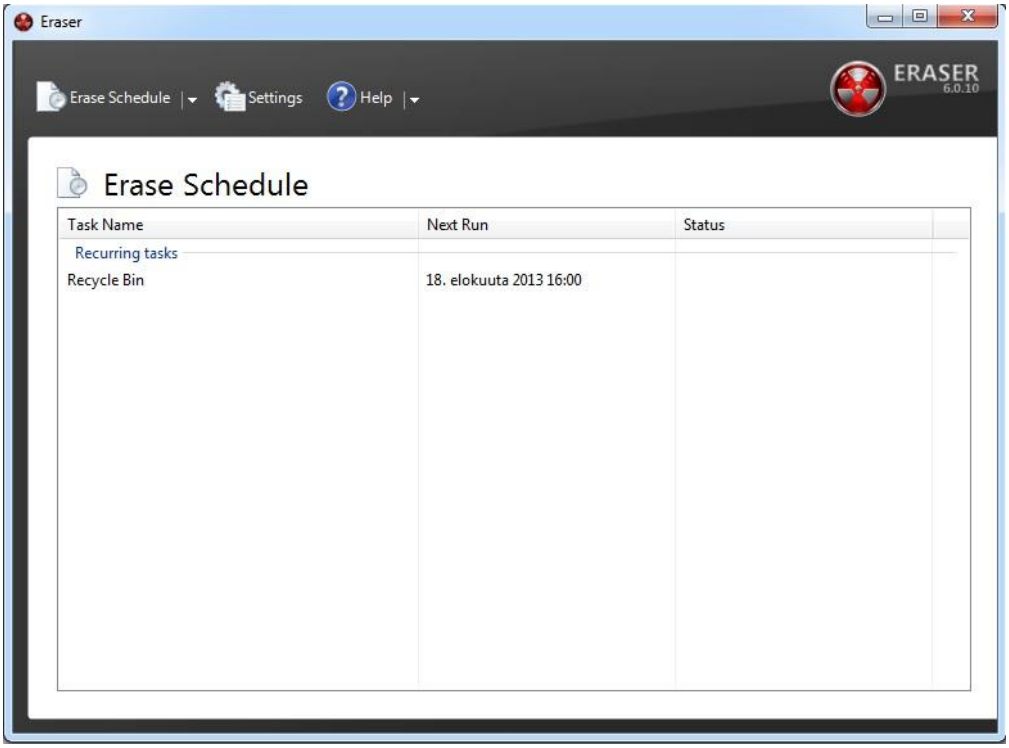
Kuva 25. Eraser, Task Type.

Valitse **Schedule** –välilehti, kirjoita haluamasi kellonaika **Run this task at:** -otsikon viereiseen kenttään ja valitse haluamasi aikaväli **Recurrence Pattern** –valikoista. Kuvassa ohjelmalle on annettu ohjeet toistaa työ joka sunnuntai klo 16 (Kuva 26).



Kuva 26. Eraser, työn aikatauluttaminen.

Lopuksi klikkaa Ok. Aikataulutettu työ näkyy nyt Eraser –sovelluksen perusnäkymässä (Kuva 27).



Kuva 27. Eraser työn lisäämisen jälkeen.